


Application Engine

磊科网络



# 7224NSW Websmart交换机

# 用户手册

# 目　　录

# 第一章 前 言

## 1.1 公司简介

衷心感谢您选用 NETCORE 产品！您将得到长期、全面和高质量的服务！

NETCORE 公司 1988 年正式成立于台湾，是新竹工业园早期创业者之一，作为国际知名的网络通信专业厂商，主要从事于局域网络、无线网络、SOHO 网络以及通讯产品研发、生产和销售。公司本着“诚信”的经营理念，依靠强大的技术背景，在 90 年代迅速崛起。目前拥有强大的研发和生产能力，分支机构遍及全球，在客户中博得广泛赞誉。

NETCORE 中国公司于 2000 年 10 月正式宣布成立，现已在中国地区设立了一个营销中心，一个生产基地和两个研发中心，并在国内主要中心城市建立了 10 多个销售办事处，辐射全国网络市场。

NETCORE 中国公司旨在为国内用户提供经济、高效、实用的全面网络解决方案，产品包括网卡、集线器、交换机、路由器、调制解调器等多个系列。并致力于三层到七层交换、全光网等前端科技的研发与应用。2000 年 11 月，NETCORE 成为首家在国内市场上推出千兆铜缆交换机的网络厂商。

“专业、优质、创新”，NETCORE 中国公司将与广大用户一起迎接信息时代的挑战！

## 1.2 用途

本手册的用途是帮助你便捷和正确地使用 Netcore 7224NSW 二层交换机。在您准备使用本产品之前，请仔细阅读本手册，以方便、快捷的使用本产品的所有功能。

## 1.3 约定

在阅读本手册时，敬请注意下列事项：


**温馨提示：**在使用交换机需要注意的一些事项


**重要提示：**在使用交换机需要特别注意的事项


**友情提示：**在使用交换机过程中必要的解释信息

## 1.4 版权、商标声明

# 第二章 认识 Netcore 7224NSW 交换机

## 2.1 产品特性

Netcore7224NSW 交换机是磊科公司新近推出的一款高性能、多用途、高安全性的二层网管型交换机。

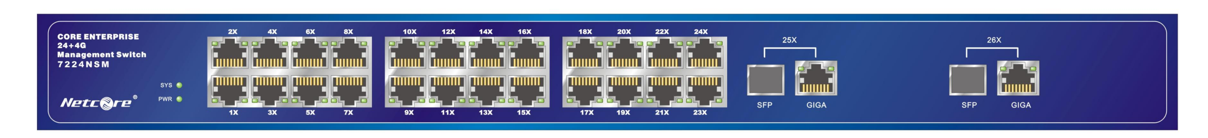



图 2.2 Netcore 7224NSW 外观示意图片

### 2.1.1 硬件特性

- 7224NSW支持8.8G背板带宽
- 10/100Mbps自适应以太网端口，完全自动侦测并适应10Mbps、100Mbps以及半双工、全双工链路，也可以根据用户的需要进行强制速率、双工设置
- 每组千兆铜缆/SFP（迷你GBIC）组合端口用于灵活的千兆铜缆或光纤骨干连接，支持光铜热切换，支持光模块热拔插
- 以太网端口自动侦测双绞线缆的类型（AUTO-MDIX），并自动适应不同类型的线缆
- IEEE 802.3x流量控制保证了数据帧可靠传输，使数据帧的传输损失率极大地降低
- 支持静态链路聚合，可以自动将多条物理链路合并成一条高速逻辑链路，同时起到了容错作用

### 2.1.2 网络协议

- 生成树协议（STP，Spanning Tree Protocol），遵从IEEE 802.1D文档规范。STP将自动断开桥接网络中的环路，并在冗余拓扑连接中发挥自动链路备份和灾难恢复作用。
- 虚拟局域网(VLAN):支持基于端口VLAN(Port-based VLAN)和802.1QVLAN(Tagged VLAN)，遵从IEEE 802.1q文档规范
- 组播窥探技术（IGMP Snooping）

### 2.1.3 网络应用

- 支持MAC地址绑定
- 支持MAC地址过滤
- 支持MAC地址学习管理
- 支持MAC地址老化管理

- 支持基于端口的捕获

## 2.1.4 支持强大 QoS 能力

Netcore 交换机提供多种流分类技术和多种 QoS 技术，包括 SQ、WRR、(这个是队列调度) Port-based、Vlan-based、Mac-based (这个为分类方式)，为各种应用的带宽保障提供需要的支持技术。

- 流分类：支持MAC优先级、VLAN优先级、支持802.1P、端口优先级。
- 流标记：802.1p是二层协议，可以为数据提供8个级别的优先级标记。
- 队列调度：Netcore 7224NSW二层网管交换机支持严格优先级队列与加权循环队列两种对列调度方式。

## 2.1.5 管理方式

- 同时支持串口和Telnet方式下的CLI (Command Line Interface) 管理配置,
- 支持基于WEB的管理
- 支持基于SNMP应用软件管理

## 2.1.6 系统升级、参数备份和恢复

- 支持基于WEB方式的固件升级
- 支持基于X-Modem的固件升级
- 用户在交换上所作的配置参数可以备份到本地存储器上，然后根据需要随时恢复任何一个备份的配置参数

# 2.2 面板布置

## 2.2.1 前面板

Netcore 7224NSW 二层交换机的前面板上有 24 个 10/100Mbps 端口、2 组 10/100/1000Mbps 铜缆/SFP (迷你 GBIC) 组合端口。

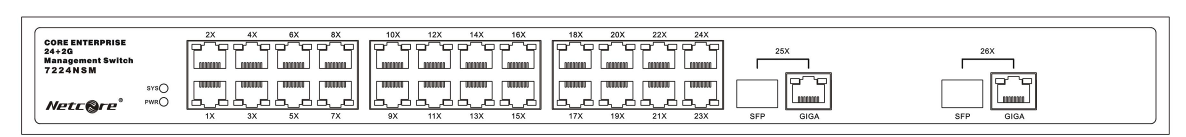



图 2.2　Netcore 7224NSW 前面板示意图片

- 10/100M Mbps自适应的UTP端口，以便与PC、服务器、其它HUB或交换机、路由器相连。支持自动线序交换的功能，与其它设备可采用交叉线或直连线进行连接。
- 交换机提供10/100/1000Mbps铜/SFP (mini GBIC) 组合千兆端口，支持光铜热切换提供

灵活的铜缆或光纤千兆连接。对于光纤连接，你可以选择适当的收发器安装在SFP插槽里来支持短、中、长距离的光缆骨干接入。使用SFP端口将会中断相应的内置10/100/1000Mbps铜缆端口的连接。

- 提供易于理解的LED状态指示灯，便于诊断网络上所发生的各种问题和故障。详见“2.2.4 LED指示灯”一节。

## 2.2.2 后面板

Netcore7224NSW 二层交换机的后面板上有 1 个电源接口、电源散热风扇，1 个 Console 控制口。

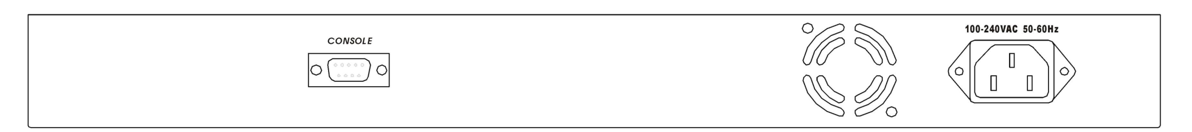



图 2.3  Netcore 7224NSW 交换机后面板示意图片

- 后面板上的交流电源接口是标准的三相接口，支持220V AC 50Hz
- 散热风扇用于进行有效的降温散热，以保证交换机的正常工作。交换机工作时请勿覆盖该通风孔
- 1个Console（RS-232）控制口，以便通过对其交换机进行管理

## 2.2.3 侧面板

Netcore 7224NSW 二层交换机的侧面板上有很多个通风孔，用于散热用途。

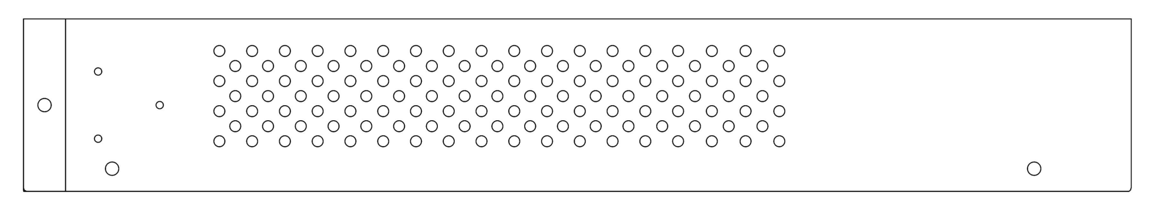


图 2.4  Netcore 7224NSW 侧面板示意图片

交换机侧面有散热风扇，用于进行有效的降温散热，以保证交换机的正常工作。交换机工作时请勿覆盖该通风孔。

## 2.2.4 LED 指示灯

通过 Netcore 7224NSW 二层交换机前面板上的 LED 指示灯，可以方便、实时地观察交换机上的各种工作状态，便于诊断所发生的问题和故障。

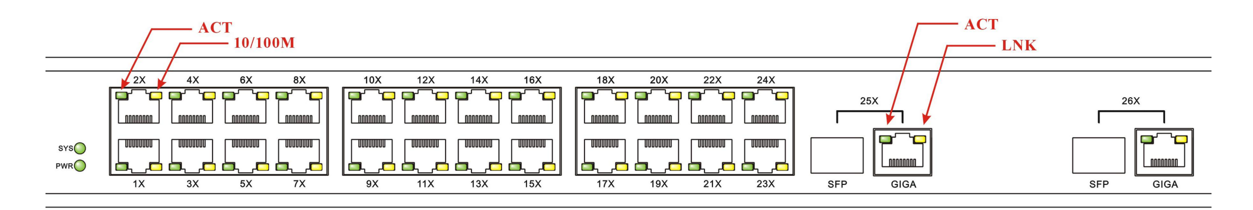



图 2.5 Netcore 7224NSW LED 指示灯示意图片

| 指示灯 | 颜色 | 描　述 |
|---|---|---|
| PWR | 绿色 | 常亮：加电正常 |
| SYS | 绿色 | 常亮：交换机里面的程序启动后，此指示灯长亮 |
| ACT | 绿色 | 常亮：建立稳定的连接 |
| 10/100M | 黄色 | 常亮：模块端口与所连接的设备以 100Mbps 速率工作<br>闪亮：有数据正在发送或者接收时 |
| | | 不亮：模块端口与所连接的设备以 10Mbps 速率工作 |
| LINK | 绿色 | 常亮：模块端口与所连接的设备以 100Mbps 速率工作<br>闪亮：有数据正在发送或者接收时 |
| | | 不亮：模块端口与所连接的设备以 10Mbps 速率工作 |

## 2.2.5 技术指标

- 端口符合标准

IEEE802.3 10BASE-T/802.3u 100BASE-TX，IEEE 802.3ab 1000Base-T 千兆以太网标准
IEEE 802.3z 1000Base-LX/SX 千兆以太网标准
ANSI/IEEE 802.3x NWay自动协商
10/100Mbps速度全/半双工
全双工IEEE 802.3x 流量控制

- 网络介质：

10Base-T – UTP/STP 3 类或 5 类双绞线
100Base-TX - UTP/STP 5 类双绞线
1000Base-T-UTP/STP 5 或 5E 类双绞线
1000Base-LX/SX 单模或多模光纤

- 端口类型

24 个屏蔽 RJ45 接口
2 个组合 10/100/1000BASE-T/SFP（mini GBIC）端口

- 迷你 GBIC（SFP）支持

IEEE802.3z 1000BASE-LX SFP 光纤模块
IEEE802.3z 1000BASE-SX SFP 光纤模块
IEEE802.3z 1000BASE-LH SFP 光纤模块
IEEE802.3z 1000BASE-ZX SFP 光纤模块

- 性能

传输方式：存储转发
MAC 地址表：每个设备 8K 条目

MAC 地址学习
动态条目:自动更新
静态条目:用户定义

- 二层包转发速率（半双工）

以太网：每端口最大线速转发 10Mbps
快速以太网：每端口最大线速转发 100Mbps
千兆以太网：每端口最大线速转发 1000Mbps

- MIBs

MIB-Ⅱ(RFC 1213)
Bridge MIB (RFC 1493)
RMON MIB (RFC1757)
802.1Q VLAN MIB (RFC 2674)
IF (Interface)MIB (RFC 2233)

- 硬件参数指标

| | 7224NSW |
|---|---|
| 工作温度 | 0℃ 到 50℃ |
| 存储温度 | -40℃ 到 70℃ |
| 工作湿度 | 10% 到 90% RH |
| 存储湿度 | 5%到 90%RH |
| 输入电源 | AC 100-240V 50-60Hz |
| 功耗 | 约 21W |
| 机械尺寸 | 432mm×250mm×44mm |
| 重量 | 3.0KG |
| 认证 | FCC PART15<br>CE |
| 噪音 | 25分贝 |

# 第三章 安装方法

## 3.1 安置方法

首先请按照下述步骤妥当地安置好交换机:

- 必须放在至少能承重4kg的表面上
- 供电的电源插座距离交换机须在1.82米之内
- 确保电源线已可靠地连接在交换机后面板上的电源接口和供电的电源插座之间
- 保证交换机的四周可以良好的通风散热并且请勿将重物放置在交换机上

## 3.2 安装在桌面上的方法

当欲将交换机安装在桌面上时，需先将包装箱内提供的 4 个黏性胶垫粘贴在交换机底面的四角的相应位置，然后，再将交换机平放在桌面上,以确保交换机的周围的空气能够良好地流动通风。

## 3.3 安装在机架中的方法

交换机可以被安装在标准的 19 英寸的机架内。首先，需要将包装箱内已提供的上机架的配件用与其配套的螺丝固定在交换机的前面板的两侧，然后，再用螺丝将交换机安装在 19 英寸的机架内。

## 3.4 加电

交换机的输入电压范围是 100-240 VAC（50-60Hz）的交流电，交换机的内置电源系统可以根据实际输入的电压自动调整其工作电压。电源接口位于交换机的后面板上，请将电源线一头插在交换机后面板上的电源接口上，另一头插在电源插座上。

交换机通电后交换机上的 LED 指示灯将会出现如下反应：

- “PWR”指示灯长亮，所有LED指示灯将快速闪亮一下。
- 当交换机在加载系统软件并进行自检时，“CPU”指示灯将闪烁。大约在60秒钟之后，“CPU”指示灯将持续长亮，表示交换机已处于工作状态。
- “10/100M”指示灯、“FDX/COL”指示灯将亮或者灭，依赖于对应模块端口的连接状态。


重要提示

当供电系统出现掉电故障时，为了确保交换机不被突发性的大电流而损坏，请务必将交换机的电源线从供电的插座上拔下来。当供电恢复正常后，再将交换机的电源线插上。

# 第四章 交换机的连接方法

## 4.1 交换机的连接

交换机前面板提供 24 个 100BASE-T RJ-45 端口，这 24 个端口能自动侦测网络速度、自动适应双工状态。可在以太网和快速以太网网络中实现 10MBps/100Mbps 传输速率（半双工模式），20MBps/200Mbps 传输速率（全双工模式）。

7224NSW 交换机提供 2 组千兆铜缆/SFP（迷你 GBIC）组合端口用于灵活的千兆铜缆或光纤骨干连接。

本交换机能够连接工作站 PC、服务器、集线器、路由器、网桥、中继器或其他交换机。

## 4.2 与网络最终节点的连接方法

连接网络终节点请用 3 类或 3 类以上的非屏蔽或屏蔽双绞线连接交换机 RJ-45 接口和网络终节点 RJ-45 接口。本交换机具有 AUTO-MDI/MDIX 自动线序交叉功能，直连线和交叉线都能连接本交换机。

在 10Base-T 以太网必须使用 3 类或 3 类以上的屏蔽或非屏蔽双绞线。

在 100Base-TX 快速以太网必须使用 5 类或 5 类以上的屏蔽或非屏蔽双绞线。

在 1000Base-T 千兆以太网必须使用 5e 类屏蔽或非屏蔽双绞线。

通过双绞线连接交换机与网络最终节点时双绞线的长度请不要超过 100 米。

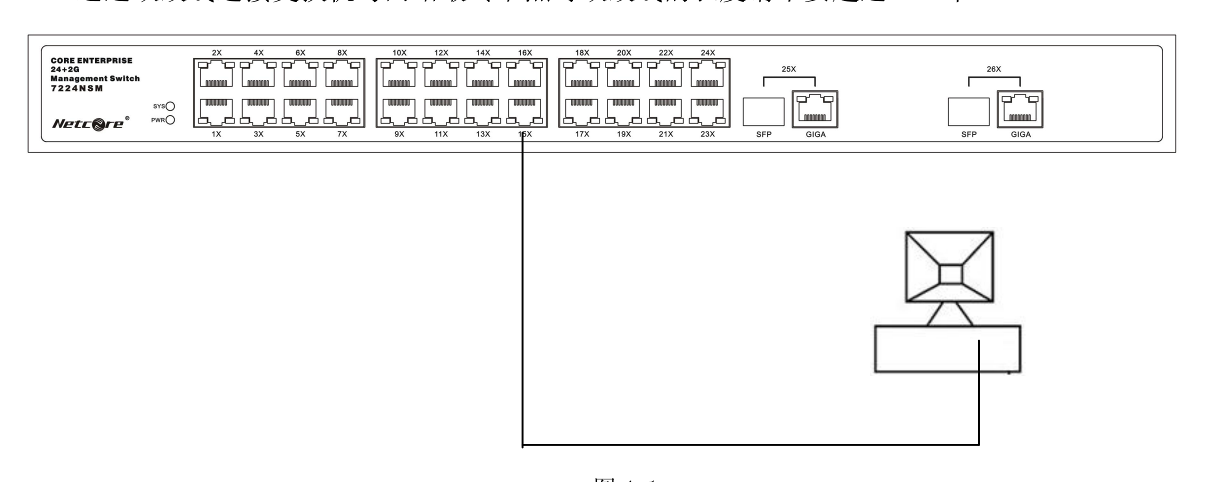



图 4.1

温馨提示

如果连接正确对应端口的 LED 指示灯将出现如下反应：

1：当所连接的设备正常连接到交换机，并且所连接的设备开机时，“ACT”指示灯将长亮

2：如果相应的 LED 指示灯不亮，请检查网卡的安装、网线的连接等是否正确。

# 4.3 与其它 HUB 或交换机的连接方法

将 Netcore 7224NSW 二层交换机与其他网络设备采用直联线或交叉线直接相连。

1:10BASE-T 的 HUB 或交换机与 7224NSW 相连时,可以使用 3 类、4 类或者 5 类或以上的 UTP/STP 双绞线。

2：100BASE-T 的 HUB 或交换机与 7224NSW 相连时，必须使用 5 类或以上的 UTP/STP 双绞线。

3：1000BASE-T的网卡或交换机与7224NSW相连时，必须使用超5e类或以上的UTP/STP双绞线。

# 第五章 配置您的交换机

## 5.1 概述

Netcore 7224NSW二层交换机可采用四种方式进行管理：

- 基于Web界面的管理（HTTP）
- 远程登录（TELNET）管理
- 控制台（CONSOLE）方式管理
- SNMP 方式管理

基于Web页面的管理方式简单易学，用户利用Microsoft Internet Explorer浏览器可以迅速对Netcore 7224NSW二层交换机进行管理配置。

远程登录（Telnet）和控制台（CONSOLE）则是以CLI方式对交换机进行管理。

SNMP方式使用第三方提供的SNMP网管软件（如：惠普的openview）进行管理。

Netcore 7224NSW二层交换机使用控制台（CONSOLE）方式进行配置。

下面分别介绍使用基于Web页面（HTTP）、远程登录（TELNET）和控制台（CONSOLE）方式进行管理的简要用法。由于第三方SNMP网管软件种类繁多，而各家使用方式各不相同，在此不作介绍。

以下的操作均在Microsoft Windows系列操作系统中进行。

## 5.2 管理方式

### 5.2.1 Web 管理方式（HTTP）

这种管理方法类似于访问一个网站，由于采用TCP/IP协议，可以实现远程管理。

首先按照下面示意图建立好TCP/IP网络连接：

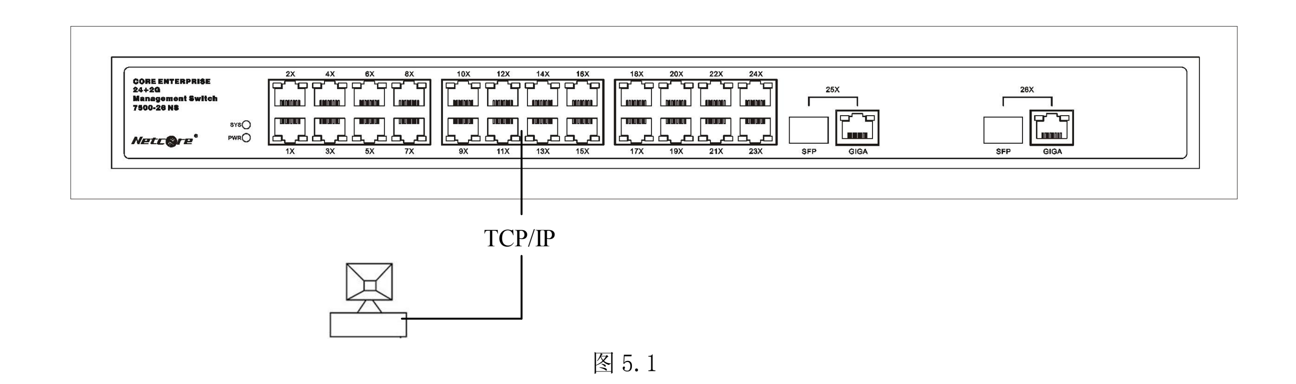



图 5.1

打开Windows系统中的Internet Explorer程序（推荐使用IE5.0以上），在地址栏里输入交换机的IP地址。


温馨提示

出厂时交换机的 IP 地址：192.168.2.11。

Netcore 7224NSW交换机的WEB登录页面，如图所示：




图 5.2

用户可以输入用户名和密码，进入交换机的WEB管理页面。


温馨提示

出厂时交换机的默认用户名为 admin，密码为 netcore。

Netcore 7224NSW二层交换机的管理主页如图5.3所示：




图 5.3　7224NSW 主页

## 5.2.2　远程登录方式（TELNET）

这种管理方法采用CLI方式，操作方式类似于控制台方式(CONSOLE)，不同的是首先要建立远程连接，并通过登录认证。由于采用TCP/IP协议，这种方式可以实现远程管理。

用户可以通过Windows提供的TELNET实用工具来建立远程连接，具体操作：点击 Windows的菜单导航条“【开始】-【运行】”，在【打开】框中输入“telnet 192.168.2.11”并确定。




第一步：

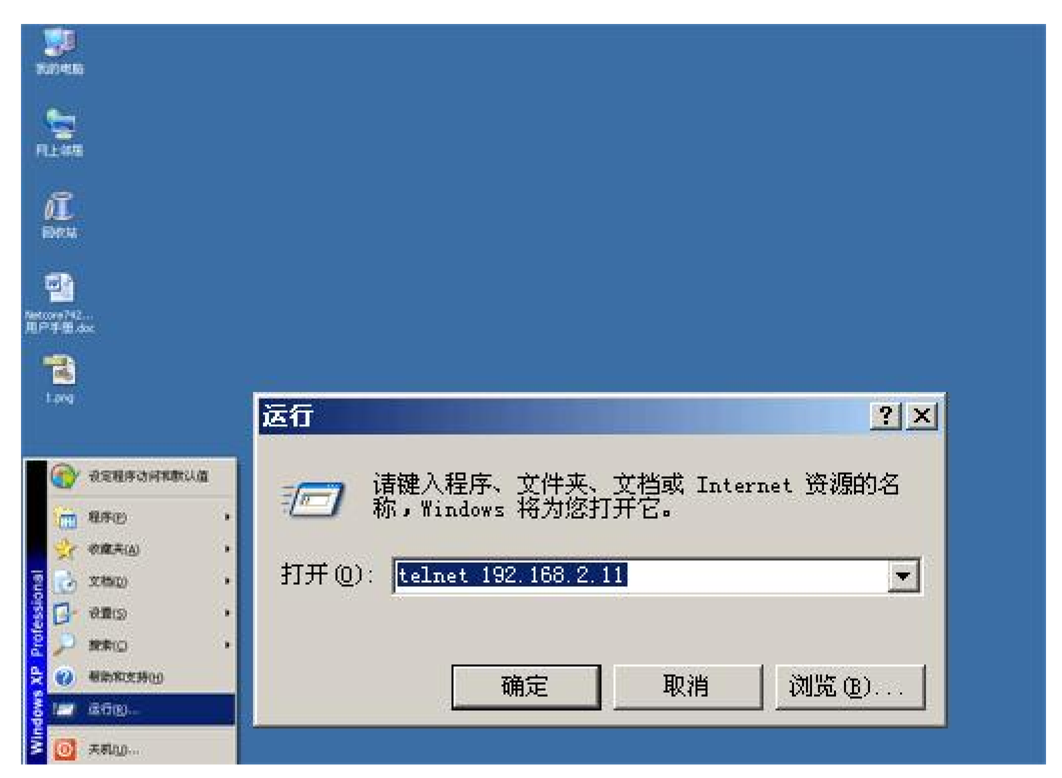



图 5.4

第二步：连接成功后，系统要求用户输入用户名和密码登陆交换机的TELNET管理页面。如图所示：

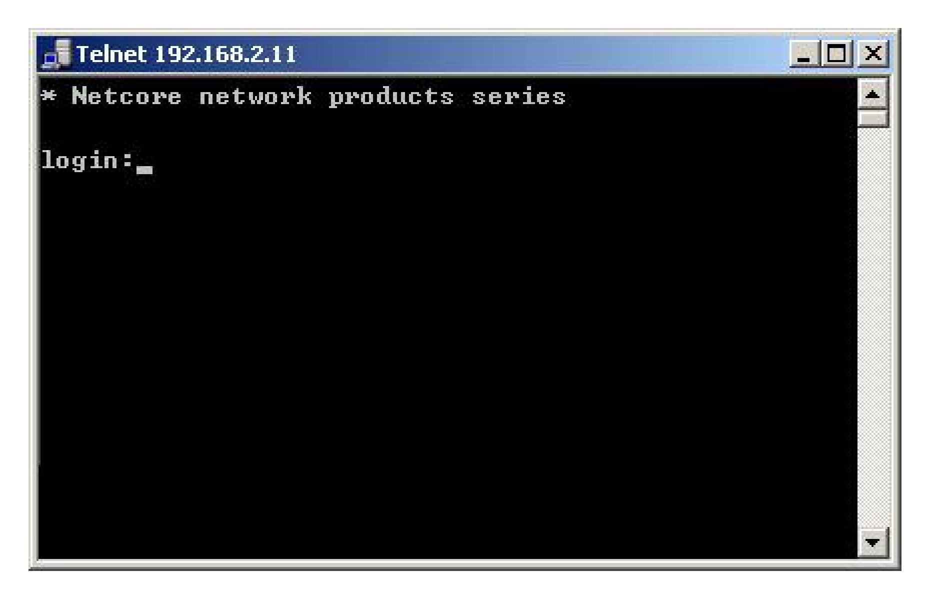
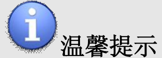



图 5.5

温馨提示

出厂时 Netcore 7224NSW 二层交换机的默认 TELNET 登陆用户名和密码：guest/guest，进入特权模式的配置密码为：netcore。

## 5.2.3 控制台方式（CONSOLE）

控制台方式是通过Microsoft Windows的超级终端对交换机进行管理和配置。这种方式可以方便地通过PC的串行口对设备进行管理，由于该方式不依赖于网络连接，所以当出现链路故障时，通常使用这种方式进行检测。

该连接方法请参考前面有关章节。

推荐用户使用Windows附带的实用程序【超级终端】来进行控制台配置工作。具体方法是：点击 【开始】-【程序】-【附件】-【通讯】-【超级终端】。

第一步：输入新建连接名称，例如netcore，如图所示：




图 5.6

第二步：选择PC上连接交换机的串行接口，并设置该串行口的通讯属性（波特率，奇偶校验，数据位，停止位，流控），如图所示：




图 5.7

温馨提示

出厂时 Netcore 7224NSW 二层交换机的 CONSOLE 端口的通讯设置为：波特率 9600，奇偶校验-无，数据位 8 位，停止位 1 位，无流控。




图 5.8



**温馨提示**

出厂时 Netcore 7224NSW 二层交换机的默认 CONSOLE 管理特权密码：netcore。

设置完成后，按确定按钮，即可对Netcore 7224NSW进行设置。

# 第六章 交换机的功能配置指南

在前面章节5.2.1我们已经详细介绍了如何使用交换机的WEB配置管理，下面以WEB配置为例具体介绍交换机各种功能的使用。介绍顺序以交换机主菜单栏为索引。

## 6.1 系统管理

### 6.1.1 IP 地址

设置Netcore 7224NSW交换机的IP地址。（默认IP地址为192.168.2.11），用户可以任意设定所需要的IP地址。

具体操作：在“IP地址”的配置页面上输入新的IP地址和子网掩码和网关地址。点击确定完成IP地址设置。配置网关地址可以使主机跨网段登陆交换机进行配置。如图所示：

| IP地址配置 | |
|---|---|
| IP地址： | 192.168.2.11 |
| 子网掩码： | 255.255.255.0 |
| 网关： | 192.168.2.1 |
| 确定 | |

图 6.1

### 6.1.2 修改密码

设置管理Netcore7224NSW二层交换机的管理密码（默认为netcore）。

具体操作：在帐户管理的设定页面上输入旧密码、新密码和确认密码。如图所示：




图 6.2

## 6.1.3 MAC 地址

设置Netcore 7224NSW二层交换机的MAC地址。

具体操作：在“MAC地址”配置页面上输入新的MAC地址。如图所示：




图 6.3

## 6.1.4 CONSOLE 信息

查看登录Netcore 7224NSW二层交换机CONSOLE口管理配置信息。如图所示：

Console 信 息

| | |
|---|---|
| 数据位: | 8 |
| 停止位: | 1 |
| 奇偶校验: | none |
| 传输流控: | none |
| 波特率(bps): | 9600 |

图 6.4

## 6.1.5 管理主机配置

通过管理主机配置限制只能设置的主机 IP 地址登录交换机进行配置。不启用该功能与交换机同一网段的主机都能同时登陆交换机进行配置。

例如：限制 IP 为 192.168.2.12 的主机才能登陆交换机进行配制。

具体操作：点击“启用管理主机配置”，在配置管理主机 IP 输入框中 192.168.2.12。




图 6.5

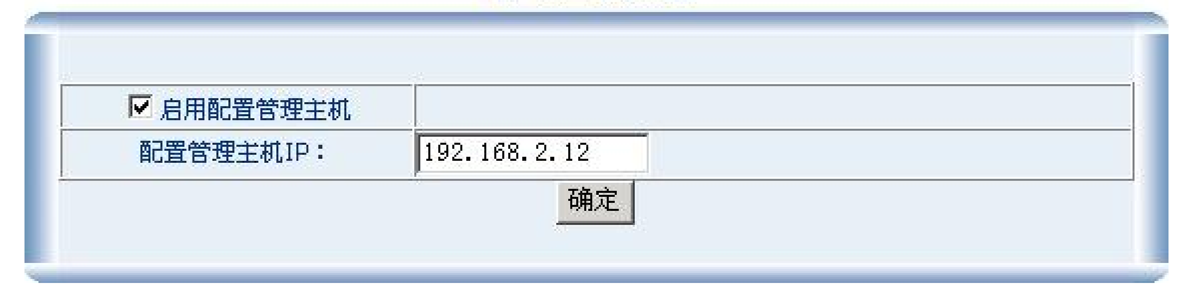



图 6.6

## 6.1.6　系统升级

通过WEB可以对Netcore 7224NSW二层交换机软件进行本地升级。点击“浏览”选中保存在本地的升级文件，然后“开始升级”当“系统升级状态”中提示升级成功后，表示用户系统升级成功。




图 6.7




## 6.1.7　参数保存

所有的参数配置好后，对Netcore 7224NSW二层交换机的配置参数进行保存，如果不作参数保存的话，当前配置的参数仅在此次配置上生效，下次重新启动后，配置的参数将会丢弃。

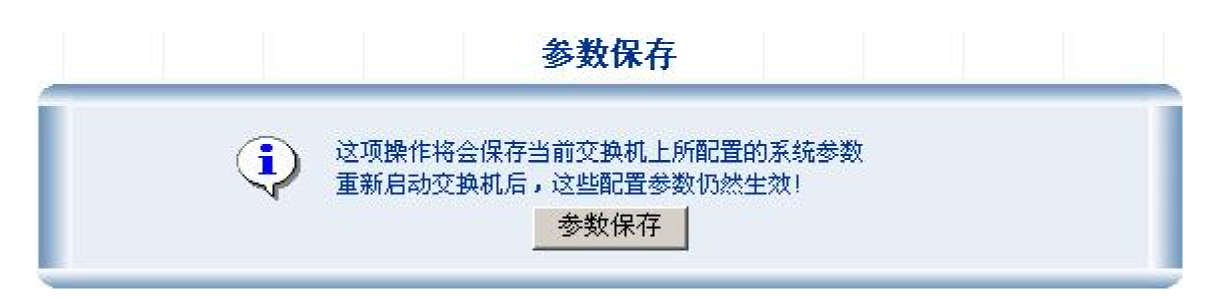



图 6.8

## 6.1.8 参数备份与恢复

- 参数备份：所有的参数配置好后，用户可以将当前Netcore 7224NSW二层交换机的配置参数进行备份，方便以后使用。
- 参数恢复：保存了的参数，用户可以任意恢复，点击“浏览”选择备份的参数文件。点击确定。当“系统参数恢复状态”显示成功时，表示用户参数恢复成功。

参数备份

备份当前交换机的所有参数配置,以便以后的恢复操作

| 参 数 恢 复 | |
|---|---|
| 系统参数文件： | 浏览... |
| 系统参数恢复状态： | |

确定

图 6.9

## 6.1.9 恢复缺省参数

恢复Netcore 7224NSW二层交换机缺省参数配置。

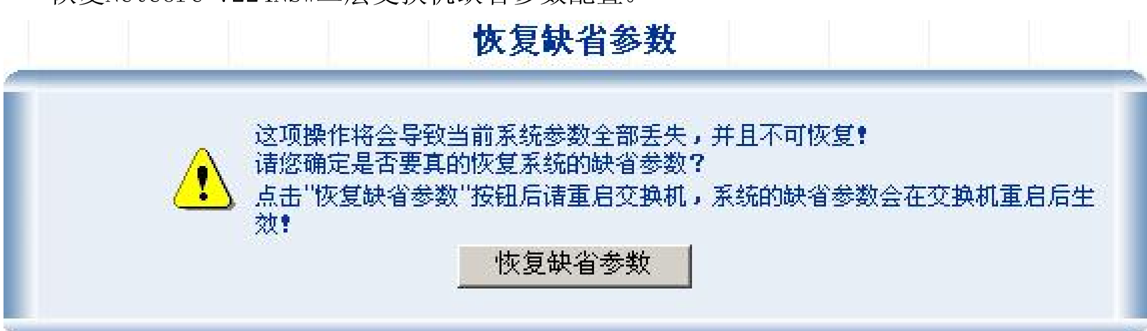



图 6.10

重要提示

此项操作将会导致交换机丢失所有当前保存的参数配置，除非遇到严重的问题，且用尽所有的故障解决方法都无效的情况下。请慎重！

## 6.2 端口管理

### 6.2.1 端口配置

用户可以自行根据需要在这里对 Netcore 7224NSW 二层交换机的各个端口进行配置。

- 端口列表：在“端口列表”框中选择要配置的端口。
- 管理状态：在“管理状态”框中可设定是否打开端口，默认为“Enable”。
- 速度/双工：在“速度/双工”框设定端口传输速度及全双工或半双工，默认为Auto。
- 流量控制：流量控制功能要求所连接的设备必须支持IEEE 802.3x且可以以全双工的方式传输，当交换机上的缓冲区被存贮满，交换机将发送Pause帧，通知发送方设备暂停发送数据。用户可通过“流量控制”框，来设定是否打开流量控制功能。

友情提示

Auto 是交换机能够自动侦测网络速度、双工状态，并根据网络情况调整自己的传输速率及双工状态以达到最高的传输速率。

端口配置的具体操作：

建议使用默认配置，也可根据情况需要自行配置。在“查看端口状态”项显示交换机当前各端口状态情况（默认配置如下图）

**端口信息**

| 端口配置 | | | |
|---|---|---|---|
| 端口列表 | 管理状态 | 速度/双工 | 流量控制 |
| port8 | Enable | Auto | Disable |

确定

| 查看端口状态 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 端口 | 管理状态 | 连接状态 | 速度 | | 双工 | | 流量控制 | |
| | | | 配置 | 实际 | 配置 | 实际 | 配置 | 实际 |
| Port 1 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 2 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 3 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 4 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 5 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 6 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 7 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 8 | Enable | Up | Auto | 100M | Auto | Full | Disable | Disable |
| Port 9 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 10 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 11 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 12 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 13 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |
| Port 14 | Enable | Down | Auto | NA | Auto | NA | Disable | NA |

图 6.11

## 6.2.2 端口统计

在“端口统计”项显示 Netcore 7224NSW 二层交换机当前各端口统计情况。交换机端口的各种流量统计显示出流量何时正常，何时有突发情况，对于网络管理员实时检测和诊断络故障是很有帮助的。

**端口统计**

| 端口 | 管理状态 | 连接状态 | 接收包总字节 | 接收包数 | 发送包总字节 | 发送包数 | 冲突包数 | 丢弃包数 |
|---|---|---|---|---|---|---|---|---|
| Port1 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port2 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port3 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port4 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port5 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port6 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port7 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port8 | Enable | Up | 352913 | 2880 | 845515 | 3386 | 0 | 0 |
| Port9 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port10 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port11 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port12 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port13 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port14 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |
| Port15 | Enable | Down | 0 | 0 | 0 | 0 | 0 | 0 |

图 6.12

# 6.3 冗余与备份

## 6.3.1 生成树

### 6.3.1.1 生成树原理

**1：关于生成树**

STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

网络中的交换机为了让其它的交换机知道它的存在而向它们传送信息包。这些信息包称为BPDU(Bridge Protocol Data Unit,网桥协议数据单元)。该信息包内主要内容是网络拓扑信息。交换机接收到这个BPDU后，便利用STA(Spanning Tree Arithmetic，生成树算法)的数学公式进行计算。通过STA计算，网桥就可以知道网络上是否存在环路。如果存在环路，网桥就作出备份端口应该被阻塞的决定，最终去出环路。

端口状态共有五种端口状态：

- 阻塞状态（Blocking）---------只侦听BPDU包，不进行数据帧转发。
- 侦听状态（Listening）--------只侦听数据帧，不进行转发。
- 学习状态（Learning）---------学习地址信息，不进行转发。
- 转发状态（Forwarding）-------学习地址信息，并进行转发。
- 无效状态（Disabled）---------不进行转发，不侦听BPDU包。因设备故障或者网络管理员的操作而导致。

通常情况下，交换机端口的状态是按照如下顺序进行转换。阻塞状态→侦听状态→学习状态→转发状态。转发状态和阻塞状态可以处于维持状态，而侦听状态和学习状态是过渡状态，最终会转换为转发状态或阻塞状态。

生成树的主要工作过程：

- 竞选根桥：启动生成树协议后，交换机之间通过传递BPDU包来交换信息。BPDU包中有一项重要信息，交换机ID。它是由8个字节组成，两个字节的优先级和6个字节的交换机的MAC地址所组成。由于MAC地址的唯一性，同样能保证交换机Id的唯一性。7224NSW交换机的优先级出厂缺省值为32768，这个数值可由网络管理员修改。因此，网路管理员可以通过控制优先级的大小来选择那个设备为根桥。网络中交换机启动生成树协议，交换机通过比较网桥ID的大小选举根网桥。协议规定，交换机ID最小的为根桥，根桥只能有一个。
- 竞选根端口：根端口是指在每个非根桥上被选择的唯一处于转发状态的端口。这个端口满足到根桥所花费的代价最小。这里所说的代价是指端口所连接的网段成本（如：全双工、半双工、10MBps网段、100MBps网段）。
- 选指定网段端口：这个过程是在每个网段上选择唯一一个指定端口。选择原则是比较网段中各端口到根桥所花费的成本，满足最小成本的端口为指定端口。其实，阶段二和阶段三是确定到根桥的最佳通路的一个过程。并且，由于三个阶段的唯一性。这样生成树协议将去掉多台交换机形成的环路。

**2：生成树相关参数**

- 最大时限（Max. Age）：最大时限的可选数值范围是6秒到40秒。在最大时限将到时，如

果还没有收到根桥发出的BPDU，那么，你的交换机将开始发送它自己的BPDU到其他所有的交换机，

- 申请成为根桥。如果你的交换机的桥标识符确实是最低的，那么，它将成为根桥。
- 呼叫时间（Hello Time）：呼叫时间的可选数值范围是1秒到10秒。这是根桥发送两个BPDU的时间间隔，告知其他所有交换机它是根桥（Root Bridge）。如果你为你的交换机设置了呼叫时间，但是它还不是根桥，那么，当你的交换机成为根桥之后，此呼叫时间就会有用处。
- 注意：呼叫时间不能比最大老化时间（Max. Age）长，否则将会出现配置错误（configuration error）的信息。
- 转发延迟时间（Forward Delay Timer）：转发延迟时间的可选数值范围是4秒到30秒。这是交换机上的端口从阻塞状态变为转发状态所需的时间。

  注: 当设置上述参数时，请一定注意下述公式：

  最大老化时间≤2×(转发时延-1 秒)

  最大老化时间≥2×(呼叫时间+1 秒)
- 桥优先级（Bridge Priority）：交换机的优先权可选数值范围是0到65535。0表示最高的优先权。
- 端口通路成本（Port Cost）：端口通路成本的可选数值范围是1 到65535。数值越小，相应的端口越可能被选定转发数据包。
- 端口优先级（Port Priority）：端口优先级的可选数值范围是0到255。数值越小，相应的端越可能成为根端口。

**3：生成树举例**

例如在一个环路中有三台交换机，如图 6.15 所示。在此例中，如果不使用生成树技术，你可以预见到可能发生的一些网络故障。例如，如果交换机 A 向交换机 B 发出一个广播包，那么，交换机 B 将把此数据包广播给交换机 C，而交换机 C 又会将此数据包广播回给交换机 A。随后会一直将如此反复，广播包将会在这个环路中被循环往复地传递，从而导致严重的网络故障。

为了避免网络环路的发生，可以如图 6.16 所示采用生成树（STP）解决。生成树将阻断交换机 B 与交换机 C 之间的连接，以打破环路的形成。生成树算法将根据计算出来的各桥和端口之间的数值，来决定断开哪一条连接。现在，如果交换机 A 向交换机 C 发出一个广播包，那么，交换机 C 将在端口 2 处将此数据包丢弃，那么此广播将结束。生成树的算法较复杂，所以，建议尽量不要改动其出厂默认设置值。生成树将自动任命根桥/根端口，并避免环路的形成。

局域网1
端口成本=19
A
端口3
桥ID=15
端口1
端口2
端口成本=4
端口成本=4
端口成本=4
端口1
B
桥ID=30
端口2
端口3
端口成本=19
C
端口1
桥ID=20
端口2
端口3
端口成本=19
端口成本=19
局域网2
局域网3

图 6.13

局域网1
A
端口3
根桥
端口1
端口2
指定端口
指定端口
根端口
根端口
端口1
B
端口2
端口3
阻塞
C
端口1
指定桥
端口2
端口3
局域网2
局域网3

图 6.14

## 6.3.1.2 Netcore 7224NSW 二层交换机生成树参数设置

**1：生成树参数配置**

- 开启生成树，将生成树默认状态设置为“Enable”。

- 各项生成树指标

  最大时限（Max Age）：(6 – 40 sec)出厂默认为 20 秒

  Hello Time: (1 – 10sec)出厂默认为 2

  转发延迟（Forward Delay）：(4 -30 sec) 出厂默认为 15

  桥优先级（Bridge Priority）：(0 – 61440) 出厂默认为 32768

用户可以根据实际状况，自行修改各项指标值。

| 生成树参数 | |
|---|---|
| 生成树状态: | Enable |
| 最大时限(Max Age,6-40s): | 20 |
| Hello时间(Hello Time,1-10s): | 2 |
| 转发延时(Forward Delay,4-30s): | 15 |
| 桥优先级(Bridge Priority,0-65535): | 32768 |
| 确定 | |

图 6.15

**2：生成树信息**

查看当前生成树各项信息。

| 生成树信息 | |
|---|---|
| 根桥优先级(Root Bridge Priority): | 32768 |
| 根桥MAC地址(Root Bridge MAC): | 00-00-01-01-02-02 |
| 根路径成本(Root Path Cost): | 0 |
| 根端口(Root Port): | 无 |
| 根桥最大时限(Root Bridge MAX age): | 20 |
| 根桥Hello时间(Root Bridge Hello Time): | 2 |
| 根桥转发时间(Root Bridge Forward Delay): | 15 |

图 6.16

**3：生成树端口参数配置**

- 在“生成树端口 参数配置”栏中，在“端口列表”中设定交换机端口号,设定是否打开快速端口，并输入端口的优先权、通路成本两项参数。
- 在“生成树端口状态”页面中查看Netcore 7224NSW交换机各端口的快速端口，通路成本，优先权三个参数的值。

| 生成树端口 参数配置 | | | |
|---|---|---|---|
| 端口列表 | 快速端口 | 通路成本(0-65535,0为Auto) | 端口优先级(0-255) |
| | Enable | | |
| 确定 | | | |

| 生成树端口状态 | | | | |
|---|---|---|---|---|
| 端口 | 快速端口 | 通路成本 | 端口优先级 | 生成树端口状态 |
| Port 1 | Disable | Auto | 0 | Forwarding |
| Port 2 | Disable | Auto | 0 | Forwarding |
| Port 3 | Disable | Auto | 0 | Forwarding |
| Port 4 | Disable | Auto | 0 | Forwarding |
| Port 5 | Disable | Auto | 0 | Forwarding |
| Port 6 | Disable | Auto | 0 | Forwarding |
| Port 7 | Disable | Auto | 0 | Forwarding |
| Port 8 | Disable | Auto | 0 | Forwarding |
| Port 9 | Disable | Auto | 0 | Forwarding |
| Port 10 | Disable | Auto | 0 | Forwarding |
| Port 11 | Disable | Auto | 0 | Forwarding |
| Port 12 | Disable | Auto | 0 | Forwarding |
| Port 13 | Disable | Auto | 0 | Forwarding |
| Port 14 | Disable | Auto | 0 | Forwarding |

图 6.17

友情提示

快速端口（Fast Port Span）特性指为了加快直接连接在用户终端（如 PC 机）或文件服务器的端口的生成树状态收敛（阻塞、侦听、学习、转发）时间，当端口的连接状态从 Linkdown 变为 Linkup 时，该端口的生成树状态马上变迁为转发状态，不需要经过侦听 / 学习过程。但如果该端口在 Linkup 后收到 BPDU，则需要参与生成树协议。而且聚合端口是不能设置为快速端口的。

## 6.3.2 链路聚合

### 6.3.2.1 链路聚合原理

链路聚合是将多个端口聚合在一起形成一个汇聚组以实现出/入负荷在各成员端口中的分担同时也提供了更高的连接可靠性。

**链路聚合的优点：**

- 通过链路聚合，可以在聚合链路的两端获得高带宽。
- 链路聚合提高了链路的可靠性，在一组链路中，如果某条物理链路失效，负载会分配到其他有效物理链路上，虽然可用带宽有所减少，但逻辑链路可以正常工作。

**链路聚合应用要求：**

- 链路聚合仅用于全双工以太网链路
- 聚合组中的所有链路，必须以同一速率工作
- 不能把聚合端口用于普通连接

### 6.3.2.2　Netcore 7224NSW 二层交换机的链路聚合方式

Netcore 7224NSW二层交换机共支持设置8个聚合组，每一个聚合组最多包括8个成员端口，设置之后，在端口列表PORT27~PORT34中。


友情提示

端口列表PORT27-PORT34表示8个聚合组。加入了聚合的端口被虚拟成一个端口，该端口的端口号为PORT27-PORT34。

### 6.3.2.3　Netcore 7224NSW 二层交换机的链路聚合配置

在下图中，我们在两台7224NSW交换机上同时设置2个端口聚合，每个端口工作在100M全双工方式下。这样配置的效果是：得到了一条双向400M带宽的逻辑链路。

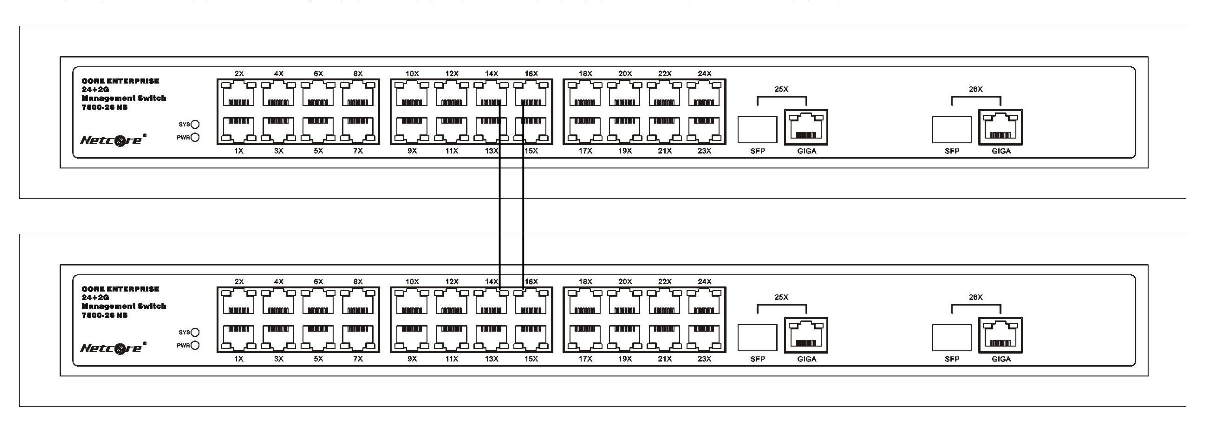


图 6.18


友情提示

Netcore7224NSW交换机支持设置12组聚合组，每组支持添加8个端口

第一步：在“链路聚合”页面中的“聚合组”中选择Port 29。（Port27-38表示为聚合组1-12）

第二步：在交换机A的链路聚合配置中，选择端口列表中的Port3、Port5,单击增加按钮，将Port3、Port5端口加入到聚合组1（Port 29）中。

第三步：在交换机B上重复第二步，将Port3，Port5加入聚合组1（Port29）。如图所示：




图 6.19

# 6.4 安全

## 6.4.1 VLAN 配置

### 6.4.1.1 VLAN（Virtual Local Area Network）的原理

它是一种通过将局域网内的设备逻辑地(而不是物理地)划分成一个个网段，从而实现虚拟工作组的技术。为了建立起安全的、独立的广播域或者组播域，可以将交换机上的端口组合成多个虚拟局域网（VLAN）。设置VLAN的主要目的是为了限制广播包的传播范围和降低广播包的影响。所有以太网数据包，如单播（unicast）、组播（multicast）、广播（broadcast）， 以及未知（unknown）的数据包，都将只在VLAN内传送。这样在一定程度上，可以提高网络的安全性。

VLAN的另一个优点是可以改变网络的拓扑结构，但并不需要网络中的工作站发生物理上的移动或者网络线路连接上的变动。可以仅仅改动工作站的VLAN设置，就可将工作站从一个VLAN（如销售部VLAN）“移到”了另一个VLAN（市场部VLAN）这可使网络节点的移动、变换、增加变得非常灵活和容易。

Netcore 7224NSW 交换机上支持两种VLAN：Port Based VLAN、802.1Q的VLAN。但在交换机上任何时刻都只能激活一种VLAN。这样，你需要选择一种最适合你的网络环境的VLAN类型来设置交换机。

IEEE 802.1QVLAN的去标记特性（untagging）使得它可以与所有合法的、无法识别VLAN标记（VLANtag）的交换机或网卡在一起工作。而IEEE802.1Q延伸到多个兼容IEEE 802.1Q的交换机上。并允许生成树（Spanning Tree）在所有端口上都能够正常地工作。

- Port Based VLAN

基于端口（port-based）的VLAN是一种简化的802.1QVLAN。基于端口的VLAN的理解和实现非常简便，如果网络管理员想快速且简易地设置VLAN，以限制广播包在网络上的传输，可选择这种最简单的基于端口的VLAN划分方法。

为了能可靠地执行VLAN的设置，请确保设备都已经直接连接在交换机上。如果是通过一台HUB、交换机或其它中继器将节点连接到交换机的端口上的，连接在该HUB、交换机或其它中继器上的所有节点都将成为该VLAN的成员。

如果想设置基于端口的VLAN，只需为其选择一个VLAN ID（交换机所有端口缺省的VID都为1），并为VLAN起一个名字，指定哪些端口属于这个VLAN就可以了，其余的端口将被自动地隔离在外。



友情提示

Netcore7224NSW交换机支持49个port-based VLAN。

- 802.1Q的VLAN

802.1Q协议，即Virtual Bridged Local Area Networks协议，主要规定了VLAN的国际标准，内容是一种在逻辑上划分网络桥接的局域网结构,并提供定义用户组在跨越不同交换设备VLAN之间的连接服务，这使得不同厂商之间的VLAN互通成为可能。VLAN的最大数目也不受交换机端口数目的限制，最大可达到4094个。

在802.1QVLAN中，网卡（NIC）不必去识别数据包头部分的802.1Q标记（tag），网卡只需发送和接收普通的以太网数据包。TAG的信息由交换机的端口根据相应的PVID加入到数据包中。交换机根据包头中的TAG信息决定如何转发这个数据包。

在理解IEEE 802.1QVLAN时，有两个非常重要的名词需要掌握，就是端口VLAN的ID（Port VLANID numbers 简写为PVID）和VLAN的ID（VLANID numbers 简写为VID）。这两个变量都是定义在端口上的，但是两者间有很大的区别。用户可以仅为每个交换机端口定义一个PVID。PVID 定义了交换机将向哪一个VLAN转发数据包，以及什么时候数据包会需要转发到另一台交换机的端口上，或者网络中的某个地方。另外，用户也可以定义某个端口同时属于多个VLAN（即VIDs），使得它可以接收网络中多个VLAN的数据包。PVID 和VID 这两个变量用于控制端口发送和接收VLAN数据流的能力，而两者之间的区别在于后者还允许信息可以在多个VLAN间共享。



友情提示

Netcore7224NSW交换机支持512个802.1Q VLAN。

### 6.4.1.2 VLAN 的相关术语

- Tagging

将802.1QVLAN的信息加入数据帧头。具有加标记能力的（tagging enabled）端口会将PVID、优先级和其它VLAN信息加入到所有进出该端口的数据帧中。如果在此前数据包已经被做过标记，端口将不对该数据包进行改动，让其保持其已有的VLAN信息。标记（Tagging）使得数据包能够从一台支持802.1Q的交换机能够传送到另一台同类的交换机上。

- Untagging

将802.1QVLAN的信息从数据帧头去掉。具有去标记能力的（untagging enabled）端口会将VID、优先级和其它VLAN信息从所有进出该端口的数据包包头中去掉。如果在此前数据包内没有被标记过,端口将不对该数据包进行改动。去标记（Untagging）使得数据包能够从一台支持802.1Q的交换机传送到其它不支持802.1Q的交换机上。

- Access 链路

即Untagging，是将802.1QVLAN的信息从数据帧头去掉。具有去标记能力的（untagging enabled）端口会将VID、优先级和其它VLAN信息从所有出该端口的数据包包头中去掉。如果在此前数据包内没有被标记过,端口将不对该数据包进行改动。去标记（Untagging）使得数据包能够从一台支持802.1Q的交换机传送到其它不支持802.1Q的交换机上。

- Trunk 链路

是将某端口设定为对某一个VLAN的数据帧Untagging，而对其他您所选定的VLAN的数据帧Tagging，Tagging是将802.1QVLAN的信息加入数据帧头。具有加标记能力的（tagging enabled）端口会将PVID、优先级和其它VLAN信息加入到所有进出该端口的数据帧中。如果在此前数据包已经被做过标记，端口将不对该数据包进行改动，让其保持其已有的VLAN信息。标记（Tagging）使得数据包能够从一台支持802.1Q的交换机能够传送到另一台同类的交换机上。

- PVID

是端口所属的VID号。

### 6.4.1.3 Netcore 7224NSW 交换机的 VLAN 设置方法

- Port Based VLAN

下列操作设置图例中的Port-based VLAN。如图所示，将Netcore7224NSW交换机的1~4端口设为VLAN2，5~8端口为VLAN3。

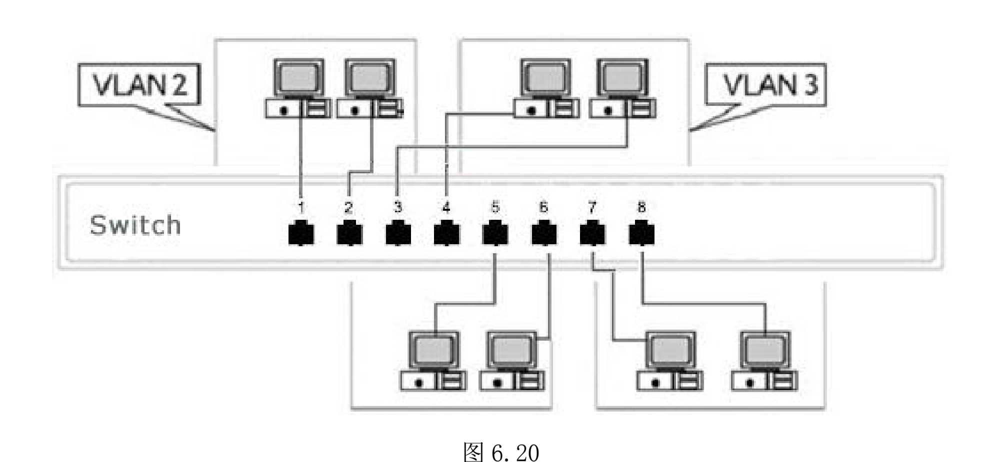



图 6.20

第一步：在VLAN配置中选中使用“port-based VLAN”点击确定。




图 6.21

第二步：“port-based VLAN”配置页面中点击“增加/修改”按钮。

Port-based VLAN

| 当前配置的VLAN | |
|---|---|
| VLAN 名称 | VID |
| vlan1 | 1 |

增加/修改

查看VLAN成员

图 6.22



友情提示

上图所示的VLAN1是交换机的默认VLAN/“Default VLAN” VID=1。在初始情况下交换机的所有端口都属于default VLAN，当该端口加入新的VLAN时，自动从default VLAN中删除。

第三步：现在开始进行将Netcore7224NSW交换机的1~4端口设为VLAN1，5~8端口为VLAN2的设置。在“VLAN名称”框输入VLAN2、“VID”框输入2，然后点击“确定”。然后选中“port1”~“port4”点击“增加”将端口加入VLAN2。

Port-based VLAN配置

VID(1-49): 2　　VLAN名称: vlan2

确定　　注意:点击确定添加一个vlan

接下来添加vlan成员端口

配置Port-based VLAN 成员端口

| 端口列表 | | VLAN成员端口 |
|---|---|---|
| Port1<br>Port2<br>Port3<br>Port4<br>Port5<br>Port6<br>Port7<br>Port8<br>Port9 | 增加<br>删除 | |

关闭

图 6.23

Port-based VLAN配置

VID(1-49): 2　　VLAN名称: vlan2

确定

配置Port-based VLAN 成员端口

| 端口列表 | | VLAN成员端口 |
|---|---|---|
| Port1<br>Port2<br>Port3<br>Port4<br>Port5<br>Port6<br>Port7<br>Port8<br>Port9 | 增加<br>删除 | Port1<br>Port2<br>Port3<br>Port4 |

注意:点击增加把相应端口添加到vlan

关闭

图 6.24

第四步：返回"图6.25"所示页面，点击"查看 VLAN成员" 可以看到已成功设置了VLAN2。



| 2 | vlan2 | Port1. | NA |
|---|---|---|---|

图 6.25



友情提示

port1-port4添加到VLAN2后，交换机自动从VLAN1中删除了port1-port4 四个端口

将"port5"～"port8"加入VLAN3的步骤同上类似。

第五步：返回"port-based VLAN"配置页面中点击Vlan名称可以进行修改Vlan配置，如下图所示。




图 6.26

- 802.1QVLAN

在支持802.1Q的交换机(802.1Q-compliant switches)之间的数据传送原理，如下图所示。

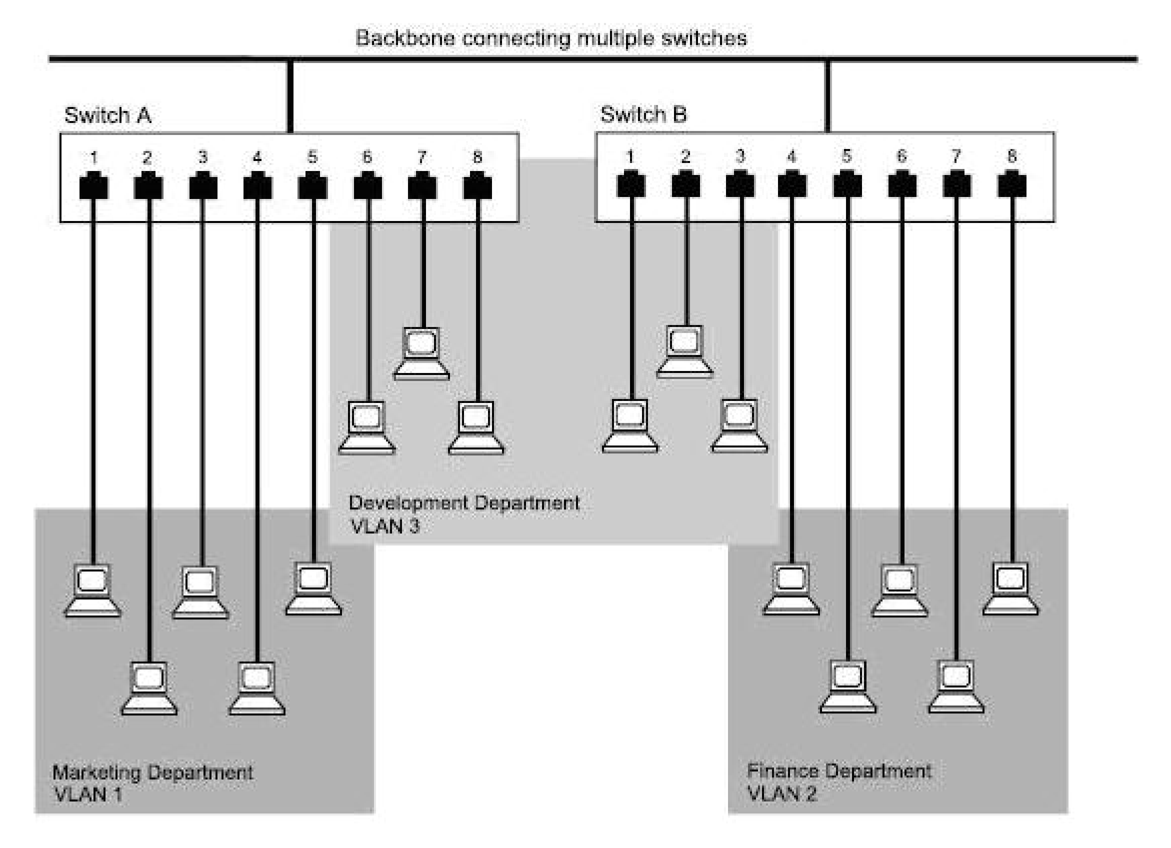



图 6.32

结合上图在Netcore7224NSW二层交换机上的具体操作：

**第一步：启用802.1Q。在VLAN配置中选中使用“802.1QVLAN”点击确定。**




图 6.33

**第二步：这时您可以看到所有端口的VLAN信息显示。**

802.1Q VLAN

| 端口 | 链路类型 | PVID | 出口规则 |
| --- | --- | --- | --- |
| Port1 | Access | 1 | Untagged=1 |
| Port2 | Access | 1 | Untagged=1 |
| Port3 | Access | 1 | Untagged=1 |
| Port4 | Access | 1 | Untagged=1 |
| Port5 | Access | 1 | Untagged=1 |
| Port6 | Access | 1 | Untagged=1 |
| Port7 | Access | 1 | Untagged=1 |
| Port8 | Access | 1 | Untagged=1 |
| Port9 | Access | 1 | Untagged=1 |
| Port10 | Access | 1 | Untagged=1 |
| Port11 | Access | 1 | Untagged=1 |
| Port12 | Access | 1 | Untagged=1 |
| Port13 | Access | 1 | Untagged=1 |

图 6.34

交换机的802.1Q的配置是基于每一个端口来配置所属VLAN的信息，首先按第三步进入端口配置该端口所属VLAN信息。

**第三步：点击您所需要设定的端口，进入设置页面。**

802.1Q VLAN

| 端口 | 链路类型 | PVID | 出口规则 |
| --- | --- | --- | --- |
| Port1 | Access | 1 | Untagged=1 <--点击此处可以修改该端口的Vlan配置 |
| Port2 | Access | 1 | Untagged=1 |
| Port3 | Access | 1 | Untagged=1 |
| Port4 | Access | 1 | Untagged=1 |
| Port5 | Access | 1 | Untagged=1 |
| Port6 | Access | 1 | Untagged=1 |
| Port7 | Access | 1 | Untagged=1 |
| Port8 | Access | 1 | Untagged=1 |
| Port9 | Access | 1 | Untagged=1 |
| Port10 | Access | 1 | Untagged=1 |
| Port11 | Access | 1 | Untagged=1 |
| Port12 | Access | 1 | Untagged=1 |
| Port13 | Access | 1 | Untagged=1 |

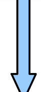


图 6.35

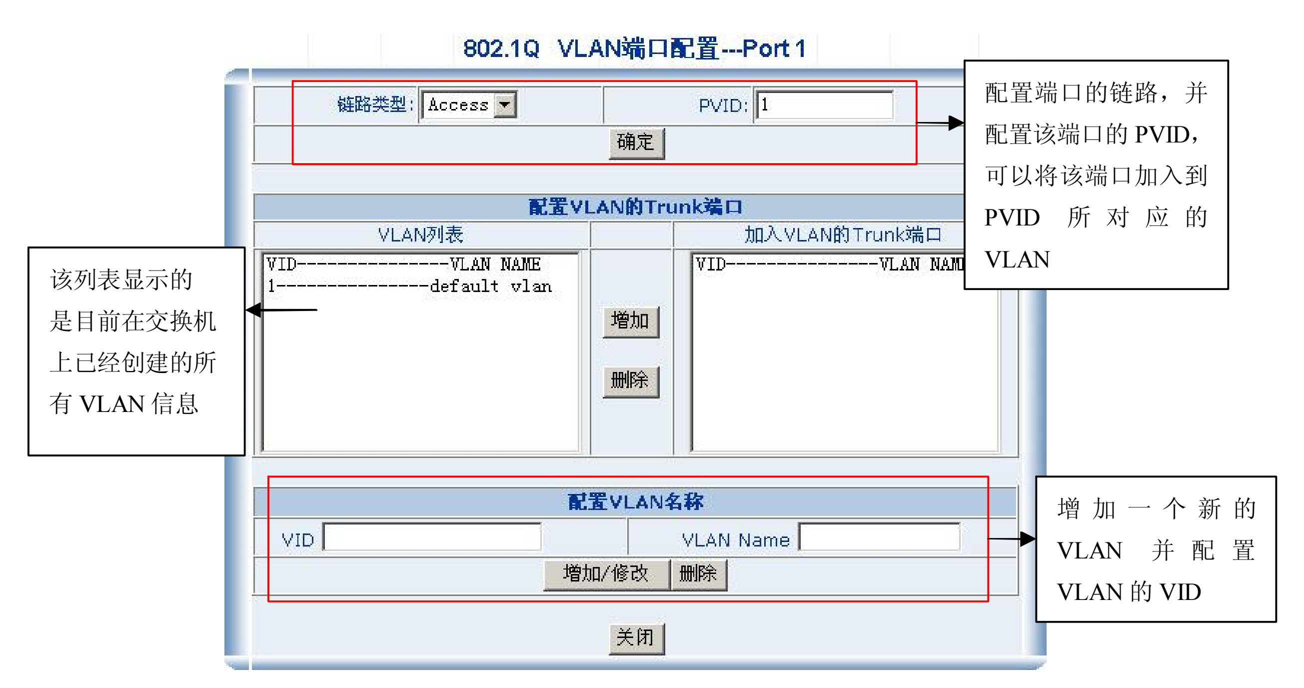



图 6.36



友情提示

上图所示的VLAN1是交换机的默认VLAN/“Default VLAN” VID=1。在初始情况下交换机的所有端口都属于default VLAN，当该端口加入新的VLAN时，自动从default VLAN中删除。

**第四步：增加一个新的VLAN**

增加VLAN。输入VLAN名称，输入VID的值，




图 6.37

新增加的VLAN会显示在VLAN列表中




图 6.38

增加了VLAN后，可以对应每个端口的配置，通过配置PVID和Trunk 端口属性，决定是否将该端口加入一个VLAN 。

**第五步：将端口加入一个VLAN**

- **配置PVID**：通过配置PVID，将端口加入一个VLAN


友情提示
交换机默认将 PVID 与 VID 与 VLAN 对应。PVID=2 相当于将一个端口设置为 VLAN2 的成员。

例如：将端口2的链路设置为ACCESS，并将port2的PVID设置为2 ，此时已经将端口2配置为VLAN2的成员




图 6.39

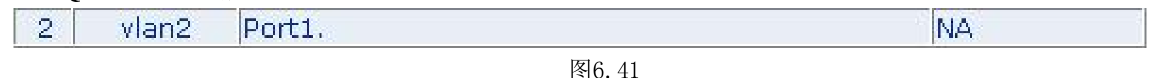
- **配置VLAN的Trunk端口**
- 在VLAN列表中选择您从该端口需要Tagging的VLAN（选中表明已经将端口加入到某个VLAN），增加到右边的“加入VLAN的Trunk端口”列表中。如果端口属于多个VLAN，没有选中的VLAN的从该端口出去时都不带tag头。

例如：选中VLAN2。，从该端口出去的VLAN2数据都必须带Tag头。




图 6.40

**第六步：返回图6.27所示页面，点击“查看VLAN成员”，查看该交换机二层交换机的802.1QVLAN成员信息。**



| 2 | vlan2 | Port1. | NA |
|---|---|---|---|

图6.41

例：PC1与PC3属于同一VLAN ；PC2与交换2上某一台机器属于同一VLAN

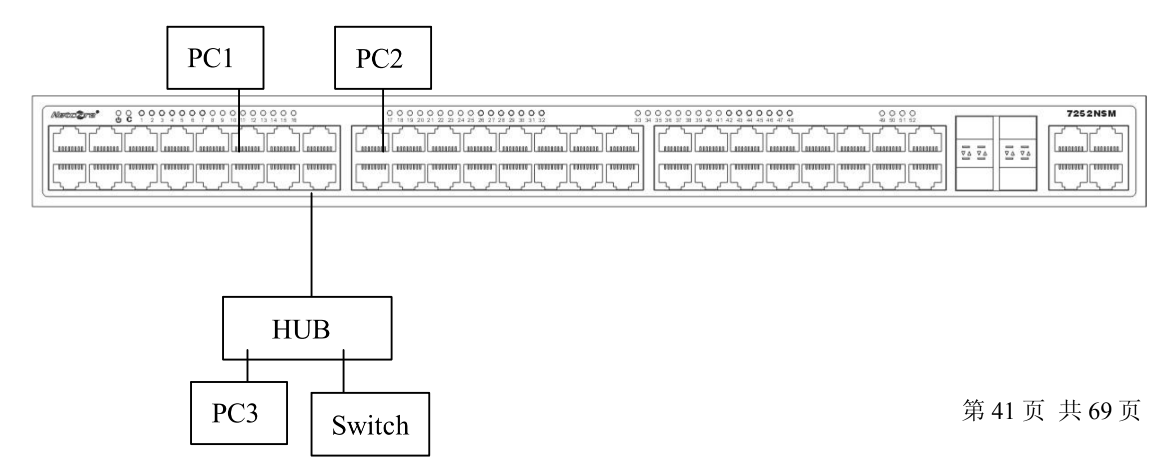


图6.42

分析：根据需求需要创建两个VLAN ：VLAN2和VLAN3 ，假设PC1在Port1上；PC2 在port3上，HUB接在Port2上。需要将端口1、2加入VLAN2；将端口2、3加入VLAN3（端口2既属于VLAN2又属于VLAN3）。并且让从端口2出去的VLAN2的数据Untagging（因为PC只能接受不带tag头的包）对VLAN3的数据tagging，也就是将Port2的链路设置为Trunk链路，即要传输带tag的包又要传输不带tag头的包。

- 首先创建VLAN2和VLAN3

| 配置VLAN名称 | | | |
|---|---|---|---|
| VID | 2 | VLAN Name | Vlan2 |
| 增加/修改 删除 | | | |

图6.43

创建VLAN3类似。

- 配置端口1

将端口1配置为VLAN2，将端口1的PVID设置为2 ，系统会自动加端口1加入VLAN2 ，因为端口1直接接PC，链路应该设置为Access

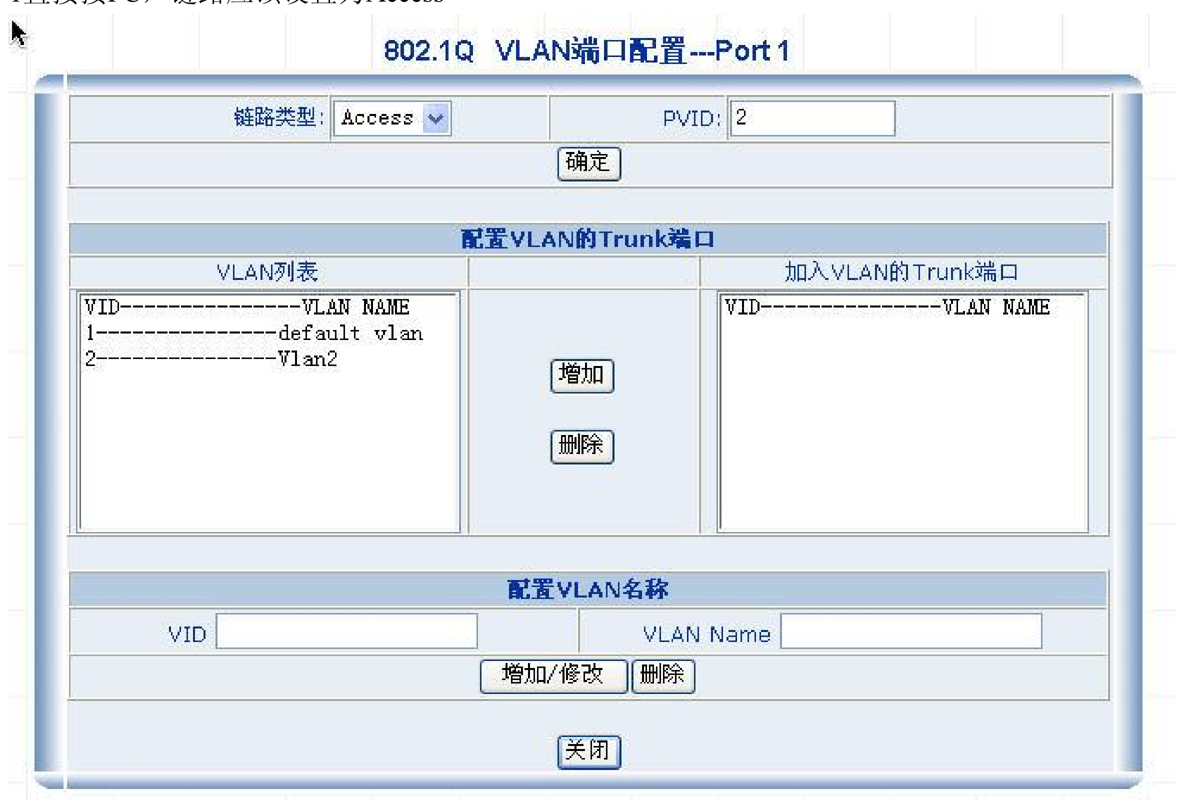



图6.44

- 配置端口3

将端口3配置为VLAN3，就是将端口3的PVID设置为3 ，系统会自动加端口3加入VLAN3 ，因为端口3直接接PC，链路应该设置为Access

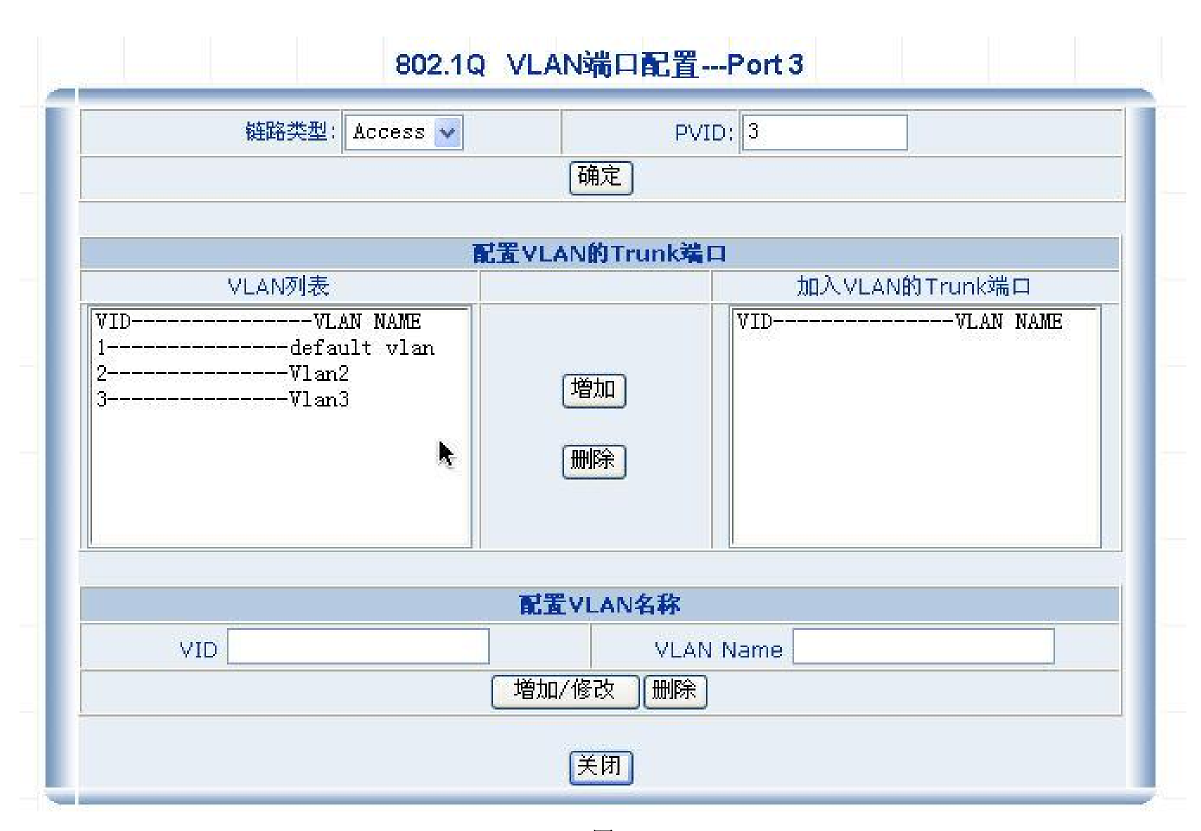



图6.45

- 配置端口2

  先将链路类型设置为Trunk。再配PVID，由于端口2同属于VLAN2和VLAN3，那么PVID应该怎么配呢？如果将PVID配置成2 ，那么系统会自动将从该端口出去的VLAN2的数据都不带tag头，而需求要求VLAN的数据是不能带tag头的，所以将PVID配置成2。需求要求VLAN3的数据要带tag，那么需要在“配置VLAN的Trunk端口”中选中VLAN3。这样VLAN3的数据从端口2出去时是带tag的数据。

802.1Q VLAN端口配置---Port 2

链路类型: Trunk　PVID: 2

确定

配置VLAN的Trunk端口

VLAN列表
VID---------------VLAN NAME
1---------------default vlan
2---------------Vlan2
3---------------Vlan3

增加　删除

加入VLAN的Trunk端口
VID---------------VLAN NAME
3---------------Vlan3

配置VLAN名称

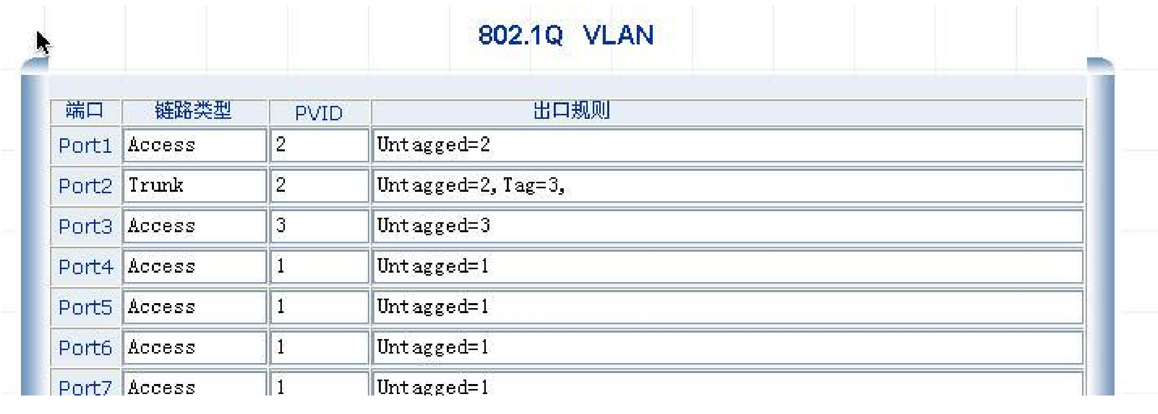
VID　VLAN Name

增加/修改　删除

关闭

图6.46

配置完成后可以去查看所有VLAN的配置信息



802.1Q VLAN

| 端口 | 链路类型 | PVID | 出口规则 |
|---|---|---|---|
| Port1 | Access | 2 | Untagged=2 |
| Port2 | Trunk | 2 | Untagged=2,Tag=3, |
| Port3 | Access | 3 | Untagged=3 |
| Port4 | Access | 1 | Untagged=1 |
| Port5 | Access | 1 | Untagged=1 |
| Port6 | Access | 1 | Untagged=1 |
| Port7 | Access | 1 | Untagged=1 |

图6.47

再查看VLAN的成员列表



查看VLAN成员

查看

| VID | VLAN名称 | VLAN成员 | VLAN Trunk端口 |
|---|---|---|---|
| 1 | default vlan | Port4.Port5.Port6.Port7.Port8.Port9.Port10.Port11.Port12.Port13.Port14.Port15.Port16.Port17.Port18.Port19.Port20.Port21.Port22.Port23.Port24.Port25.Port26.Port27.Port28. | NA |
| 2 | Vlan2 | Port1.Port2. | NA |
| 3 | Vlan3 | Port2.Port3. | Port2. |

关闭

图6.48

## 6.4.2 MAC 地址绑定

### 6.4.2.1 MAC 地址绑定原理

MAC地址绑定是Netcore 7224NSW二层交换机支持的一项基于端口的安全技术。一般情况下，MAC地址表是交换机根据所连接的网络设备，通过源地址学习自动建立起来，但网络管理员也可以手动在表中加入特定网络设备的MAC地址,使之与交换机的相应的端口绑定，被绑定后的网络设备只能通过绑定了的交换机端口访问交换机，这样就大大提高端口安全性。

### 6.4.2.2 Netcore 7224NSW 交换机的 MAC 地址绑定配置

例如：将一台MAC地址为00-E0-4F-48-3A-7E的设备限制在7224NSW的1号端口上使用，具体操作如下：

在“MAC地址”框中输入00-E0-4F-48-3A-7E，然后在“端口号”框选中“PORT1”，点击“增加”。




图6.43

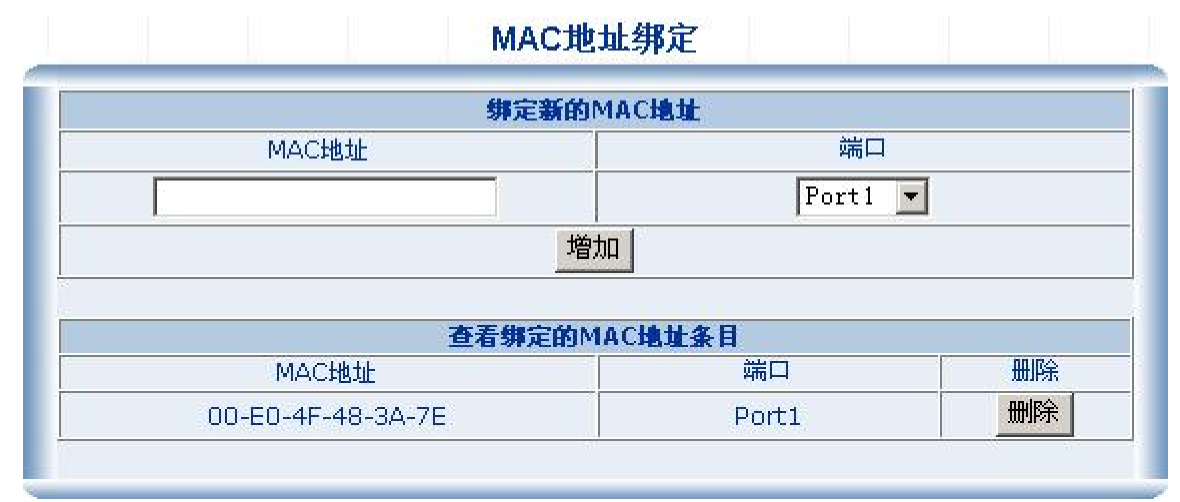



图 6.44

# 6.4.3 MAC 地址过滤

## 6.4.3.1 MAC 地址过滤原理

MAC地址过滤是交换机的另一项网络安全技术。用户可以自行把网络设备的MAC地址添加到MAC地址过滤表中，被添加到MAC地址过滤表中的网络设备将无法访问交换机。

## 6.4.3.2 Netcore7224NSW 交换机的 MAC 地址过滤配置

把连接在7224NSW交换机的一台PC的MAC地址（PC网卡的MAC地址为00-E0-4F-48-3A-7E）进行过滤，具体操作如下：

在“MAC地址”框中输入00-E0-4F-48-3A-7E，点击“增加”，如下图所示：

MAC地址过滤

过滤新的MAC地址

MAC地址

00-E0-4F-48-3A-7E

增加

当前过滤的MAC地址

| MAC地址 | 删除 |
| --- | --- |

图 6.45




图 6.46

## 6.4.4 MAC 地址老化

### 6.4.4.1 MAC 地址学习原理

MAC地址学习是Netcore 7224NSW二层交换机的另一项网络安全技术。用户可以自行选择针对每一个端口开启和关闭MAC地址学习。

### 6.4.4.2 Netcore 7224NSW 交换机的 MAC 地址学习配置

在端口列表中输入需要进行管理的端口号，在“MAC地址学习”中选择该端口的学习状态Enable/Disable。

MAC地址学习

| MAC地址学习 | |
|---|---|
| 端口列表 | MAC地址学习 |
| | Disable |
| 增加 | |

| 察看端口MAC地址学习 | |
|---|---|
| 端口 | MAC地址学习 |
| Port1 | Enable |
| Port2 | Enable |
| Port3 | Enable |
| Port4 | Enable |
| Port5 | Enable |
| Port6 | Enable |
| Port7 | Enable |
| Port8 | Enable |
| Port9 | Enable |
| Port10 | Enable |
| Port11 | Enable |
| Port12 | Enable |
| Port13 | Enable |
| Port14 | Enable |

图 6.47

## 6.4.5 MAC 地址老化

MAC条目在交换机中如果一直未激活或未触发，在此可以设定MAC地址条目在交换机中的生存时间，单位“秒”。




图 6. 48




Netcore 7224NSW二层交换机的MAC地址老化时间默认为300S。

# 6.5 QoS

## 6.5.1 QoS 简介

传统的分组网络对所有报文都无区别的等同对待。每个交换机/路由器对所有的报文采用先入先出的策略FIFO处理，尽最大的努力Best-Effort将报文送到目的地，但对报文传送的延时、延时抖动等传输性能不提供任何承诺和保证。

随着计算机网络的高速发展，对带宽、延迟、抖动敏感的语音、图像、重要数据越来越多地在网上传输。这样一方面使得网上的业务资源极大地丰富，另一方面则由于经常遭遇网络拥塞，人们对网络传输的服务质量QoS Quality of Service提出了更高的要求。

以太网技术是当今被广泛使用的网络技术。目前，以太网不仅成为各种独立的局域网中的主导技术，许多以太网形式的局域网也成为了Internet 的组成部分。而且随着以太网技术的不断发展，以太网接入方式也将成为广大普通Internet 用户的主要接入方式之一。因此要实现端到端的全网QoS解决方案，不可避免地要考虑以太网上的QoS业务保证的问题。这就需要以太网交换设备应用以太网QoS技术，对不同类型的业务流提供不同等级的QoS保证。尤其是能够支持那些对延时和抖动要求较高的业务流。

### 6.5.1.1 QoS 相关术语和概念

- **流：**流即业务流traffic 指所有通过交换机的报文。
- **流分类：**流分类traffic classification是指采用一定的规则识别出符合某类特征的报文。分类规则classification rule指配置管理员根据管理需求配置的规则。分类规则很简单，一般的分类依据都局限在封装报文的头部信息。
- **优先级标记：**以太网交换机可为特定报文提供优先级标记的服务，标记内容包括TOS、DSCP 802.1p等这些优先级标记分别适用于不同的QoS模型在不同的模型中被定义。
- **队列调度：**当网络拥塞时，必须解决多个报文同时竞争使用资源的问题。通常采用队列调度加以解决。这里介绍3种各具特色的队列调度算法：严格优先级SP（Strict-Priority）加权平均优先级（WRR：Weighted Round Robin）调度算法。

下面用简单的例子对比了在网络发生拥塞时，报文在无QoS保证和有QoS保证网络中的不同处理过程。

- 下图所示为发生拥塞时，网络设备的一个接口在不支持QoS的情况下，报文的发送情况：

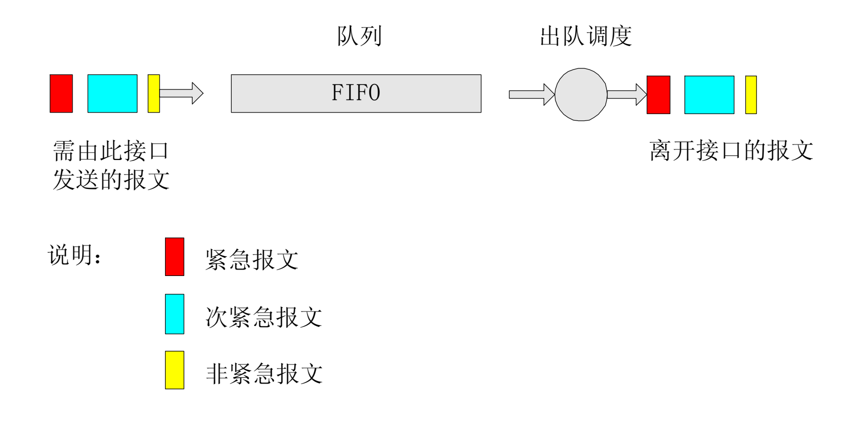



图 6.49

所有要从该接口输出的报文，按照到达的先后顺序进入接口的FIFO队列尾部，而接口在发送报文时，从FIFO（First in First out，先入先出）队列的头部开始，依次发送报文，所有的报文在发送过程中，没有任何区别，也不对报文传送的质量提供任何保证。

- 下图是一个用SQ（Strict Queuing）优先队列来支持QoS的报文发送情况：

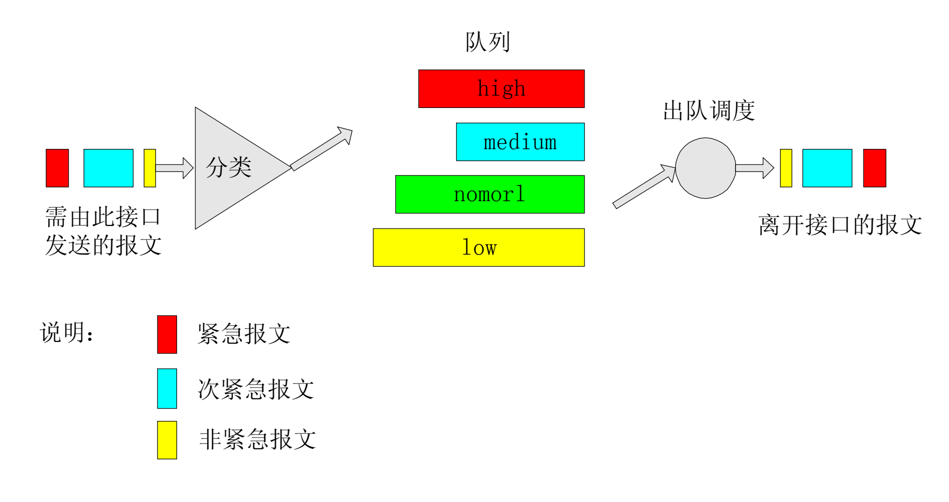



图 6.50

在报文到达接口后，首先对报文进行分类，然后按照报文所属的类别让报文进入所属队列的尾部，在报文发送时，按照优先级，总是在所有优先级高的队列发送完毕后，再发送低优先级队列中的报文。这样在每次发送报文时，总是将优先级高的报文先发出去，保证了属于较高优先级队列的报文有非常低的时延，其报文的丢失率和通过率这两个性能指标在网络拥塞时也可以有一定的保障。

- 下图是一个用WRR（Weighted Round Robin）加权平均优先级队列支持QoS的报文发送情况：

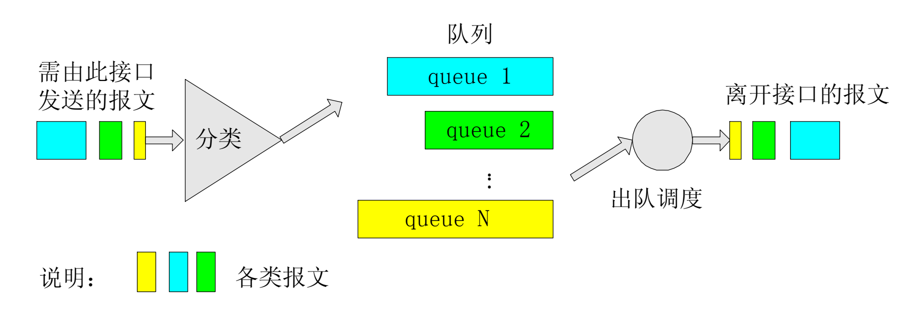



图6.51

WRR是按照对列的权重进行对列调策略，对列对应的权重越大，该队列中的数据包越能优先转发，这在保证公平的基础上对不同优先级的业务体现优先转发的特性。

QoS旨在针对各种应用的不同需求，为其提供不同的服务质量，例如：提供专用带宽、减少报文丢失率、降低报文传送时延及时延抖动等。为实现上述目的，QoS提供了下述功能：

- 报文分类和着色
- 避免和管理网络拥塞
- 流量监管和流量整形
- QoS信令协议

#### 6.5.1.2 QoS 的应用

QoS可以控制各种网络应用和满足各种网络应用要求，如：

- 控制资源：如可以限制骨干网上FTP使用的带宽，也可以给数据库访问以较高优先级。
- 可裁剪的服务：对于ISP（Inernet Service Provider，Internet服务提供商），其用户可能传送语音、视频或其他实时业务，QoS使ISP能区分这些不同的报文，并提供不同服务。
- 多种需求并存：可以为时间敏感的多媒体业务提供带宽和低时延保证，而其他业务在使用网络时，也不会影响这些时间敏感的业务。

在一个网络中，需要以下的三个部分来完成端到端的QoS：

- 各网络元件（路由器、以太网交换机等）支持QoS，提供队列调度、流量整形等功能。
- 信令技术来协调端到端之间的网络元件为报文提供QoS。
- QoS控制和管理端到端之间的报文在一个网络上的发送。而每个网络元件提供如下功能：
- 报文分类，对不同类别的报文提供不同的处理。
- 队列管理和调度来满足不同应用要求的不同服务质量。
- 流量监管和流量整形限制和调整报文输出的速度。
- 接入控制来确定是否允许用户信息流使用网络资源。

### 6.5.2 QoS 配置

Netcore 7224NSW二层网管交换机支持802.1P、端口优先级、VLAN优先级、MAC优先级多种流分类技术；支持四个优先级队列；支持严格优先级队列与加权循环队列两种对列调度方式。



友情提示

流分类技术优先级：MAC优先级、VLAN优先级、支持802.1P、端口优先级

### 6.5.2.1 MAC-COS 映射

用户可以基于MAC地址提供不同等级的优先级。



友情提示

COS即交换机转发数据使用的优先级分类，“CoS”的范围为0-7，“7”为最高优先级。针对交换机的四种流分类技术，交换机提供了COS和四种流分类技术的映射设置。

例如：对MAC地址为00-E0-4F-48-3A-7E的设备进行QOS的配置

具体操作：在“MAC地址”框中输入00-E0-4F-48-3A-7E，在“CoS”输入框中输入映射的优先级。点击确定完成配置。




图 6.52




图 6.53

## 6.5.2.2 VLAN-CoS 映射

交换机对VID值优先级映射成CoS值作为流分类的条件。
具体操作：VLAN对应的VID值，选择映射的CoS优先级，点击确定完成配置。

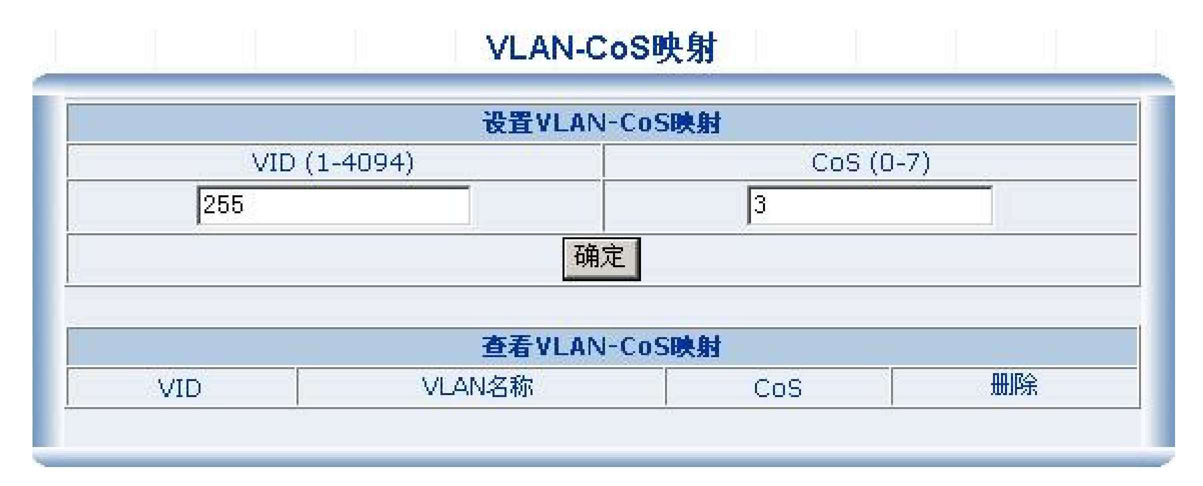



图 6.54




图 6.55

## 6.5.2.3 802.1p-priority-CoS 映射

交换机对802.1P数据帧中携带的优先级字段映射成CoS值作为流分类的条件
具体操作：在“802.1p Priority (0-7)”输入框中输入优先级分类，选择映射的CoS优先级，点击确定完成配置。

## 802.1p-priority-CoS映射

| 设置802.1p-priority-CoS映射 | |
|---|---|
| 802.1p Priority (0-7) | CoS (0-7) |
| 2 | 3 |
| 确定 | |

| 查看802.1p-priority-CoS映射 | |
|---|---|
| 802.1p Priority | CoS |
| 0 | 0 |
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |

图 6.56



## 802.1p-priority-CoS映射

| 设置802.1p-priority-CoS映射 | |
|---|---|
| 802.1p Priority (0-7) | CoS (0-7) |
| | |
| 确定 | |

| 查看802.1p-priority-CoS映射 | |
|---|---|
| 802.1p Priority | CoS |
| 0 | 0 |
| 1 | 1 |
| 2 | 3 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |

图 6.57

### 6.5.2.4 端口-CoS映射

交换机对于所有在这个端口接收的报文将以端口的CoS值作为流分类的条件。

具体操作：输入进行优先级设置的端口号，输入COS值。

**Port-based Qos**

| 设置port-based Qos | |
|---|---|
| 端口列表 | CoS (0-7) |
| 4 | 5 |
| 确定 | |

| 查看port-based Qos配置 | |
|---|---|
| 端口 | CoS |
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |
| 6 | 0 |
| 7 | 0 |
| 8 | 0 |
| 9 | 0 |
| 10 | 0 |
| 11 | 0 |
| 12 | 0 |

图6.58




图 6.59

### 6.5.2.5　CoS-Queue 映射

交换机转发数据的使用的优先级分类到队列调度的映射。
具体操作：输入进行映射COS的值，输入映射Queue队列的值。




| CoS | Queue |
|---|---|
| 0 | 0 |
| 1 | 0 |
| 2 | 1 |
| 3 | 1 |
| 4 | 2 |
| 5 | 2 |
| 6 | 3 |
| 7 | 3 |

图 6.60

### 6.5.2.6　队列调度

**1：队列调度的概念**

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题。通常采用队列调度加以解决。这里介绍2种各具特色的队列调度算法：严格优先级SP（Strict-Priority） 队列调度算法加权轮循WRR Weighted Round Robin调度算法和带最大时延的WRR 调度算法。

- SP 调度算法

SP 队列调度算法是针对关键业务型应用设计的关键业务有一重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以端口有4个输出队列为例优先队列将端口的4个输出队列分成4 类分别为高优先队列中优先队列正常优先队列和低优先队列（依次为3 2 1 0队列），它们的优先级依次降低。在队列调度时，SP严格按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样，将关键业务的分组放入较高优先级的队列，将非关键业务如E-Mail的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

SP 的缺点是拥塞发生时如果较高优先级队列中长时间有分组存在那么低优先级队列中的报文就会由于得不到服务而“饿死”。

- WRR 调度算法

交换机的端口支持8个输出队列，WRR队列调度算法在队列之间进行轮流调度保证每个队列都得到一定的服务时间。WRR 队列还有一个优点是，虽然多个队列的调度是轮循进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

**2：Netcore 7224NSW 二层交换机队列调度的设置**

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。

交换机依据报文的COS优先级进行入队列操作。

严格优先级队列SQ保证高优先级业务总是在低优先级业务之前处理；WRR是一种加权循环队列调度

机制，首先处理高优先级，但在处理高优先级业务时，较低优先级的业务并没有被完全阻塞，而是按一定的比例同时进行。Netcore 7224NSW二层交换机允许严格优先级队列与加权循环队列同时存在。




图6.61

# 6.6 组播管理

## 6.6.1 IGMP Snooping

### 6.6.1.1 组播概述

当信息（包括数据、语音和视频）传送的目的地是网络中的少数用户时，可以采用多种传送方式。可以采用单播（Unicast）的方式，即为每个用户单独建立一条数据传送通路；或者采用广播（Broadcast）的方式，把信息传送给网络中的所有用户，不管他们是否需要，都会接收到广播来的信息。例如，在一个网络上有200个用户需要接收相同的信息时，传统的解决方案是用单播方式把这一信息分别发送200次，以便确保需要数据的用户能够得到所需的数据；或者采用广播的方式，在整个网络范围内传送数据，需要这些数据的用户可直接在网络上获取。这两种方式都浪费了大量宝贵的带宽资源，而且广播方式也不利于信息的安全和保密。

IP组播技术的出现及时解决了这个问题。组播源仅发送一次信息，组播路由协议为组播数据包建立树型路由，被传递的信息在尽可能远的分叉路口才开始复制和分发（参见下图），因此，信息能够被准确高效地传送到每个需要它的用户。

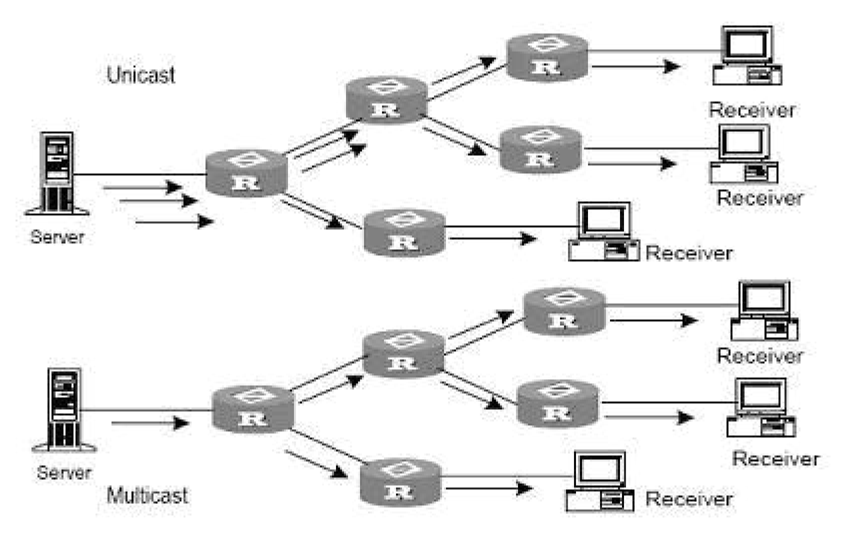



图 6.62

需要注意的是，组播源不一定属于组播组，它向组播组发送数据，自己不一定是接收者。可以同时有多个源向一个组播组发送报文。网络中可能有不支持组播的路由器，组播路由器可以使用隧道方式将组播包封装在单播IP包中传送给相邻的组播路由器，相邻的组播路由器再将单播IP头剥掉，然后继续进行组播传输。从而避免对网络的结构进行较大的改动。

**组播的优势：**

- 提高效率：降低网络流量，减轻服务器和CPU负荷；
- 优化性能：减少冗余流量；
- 分布式应用：使多点应用成为可能。

### 6.6.1.2 IGMP Snooping 原理

IGMP Snooping（Internet Group Management Protocol Snooping）是运行在二层以太网交换机上的组播约束机制，用于管理和控制组播组。

IGMP Snooping运行在链路层。当二层以太网交换机收到主机和路由器之间传递的IGMP报文时，IGMP Snooping分析IGMP报文所带的信息。当监听到主机发出的IGMP主机报告报文（IGMP host report message）时，交换机就将与该主机加入到相应的组播表中；当监听到主机发出的IGMP离开报文（IGM Pleave message）时，交换机就将删除与该主机对应的组播表项。通过不断地监控IGMP报文，交换机就可以在二层建立和维护MAC组播地址表。之后，交换机就可以根据MAC组播地址表进行转发从路由器下发的组播报文。

没有运行IGMP Snooping时，组播报文将在二层广播。如下图所示：

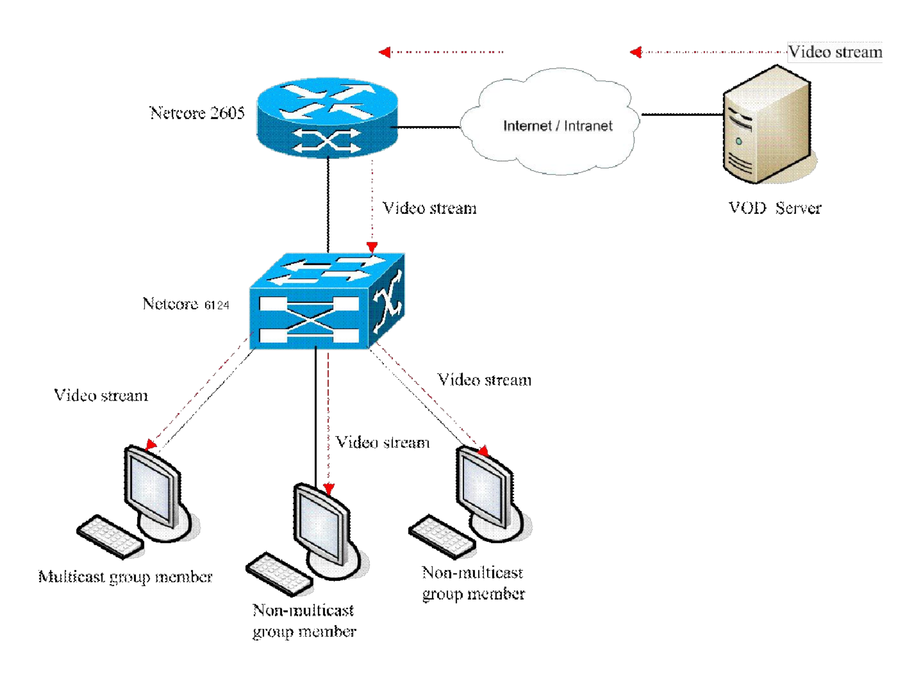



图 6.63

运行IGMP Snooping后，报文将不再在二层广播，而是进行二层组播。如下图所示：

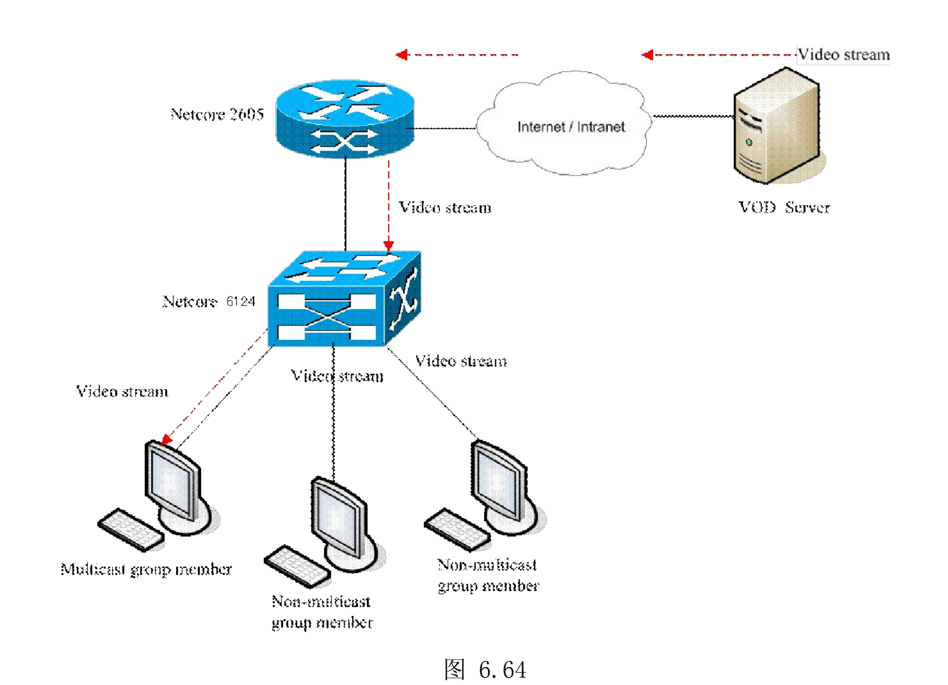



图 6.64

### 6.6.1.3 IGMP Snooping 的实现二层组播

以太网交换机通过运行IGMP Snooping实现对IGMP报文的侦测，并为主机及其对应端口与相应的组播组地址建立映射关系。为实现IGMP Snooping，二层以太网交换机对各种IGMP报文的处理过程如下：

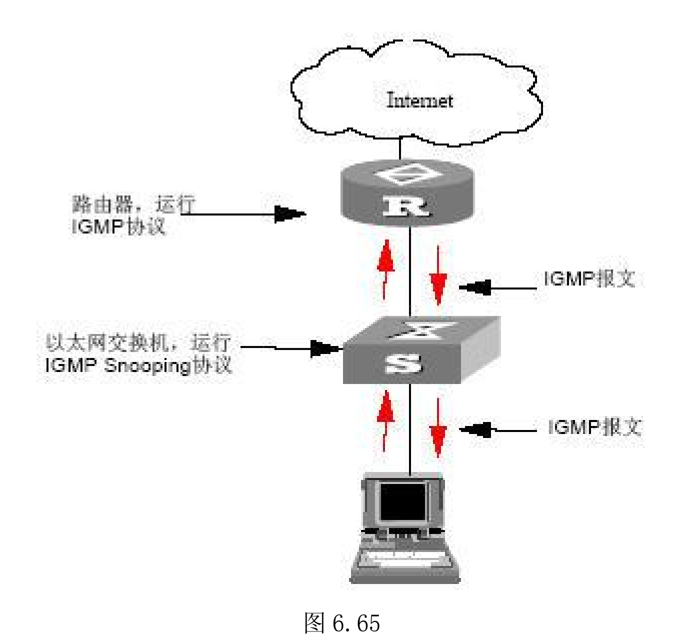



图 6.65

- IGMP通用查询报文：IGMP通用查询报文是组播路由器向组播组成员发送的报文，用于查询哪些组播组存在成员。当收到IGMP通用查询报文时，如果收到通用查询报文的端口原来就是路由器端口，以太网交换机就重置该路由器端口的老化定时器；如果收到通用查询报文的端口原来不是路由器端口，则交换机通知组播路由器有成员需要加入某个组播组，同时启动对该路由器端口的老化定时器。
- IGMP特定组查询报文：IGMP特定组查询报文是组播路由器向组播组成员发送的报文，用于查询特定组播组是否存在成员。当以太网交换机收到IGMP特定组查询报文时，只向被查询的IP组播组发特定组查询。
- IGMP报告报文：IGMP报告报文是主机向组播路由器发送的报告报文，用于申请加入某个组播组或者应答IGMP查询报文。当以太网交换机收到IGMP报告报文时，首先判断该报文要加入的IP组播组对应的MAC组播组是否已经存在。如果对应的MAC组播组不存在，只是通知路由器有成员加入某个组播组，则会新建MAC组播组，将接收报告报文的端口加入该MAC组播组中，并启动该端口的老化定时器，然后将该端口所属VLAN下存在的所有路由器端口加入到此MAC组播转发表中，同时新建IP组播组，并将接收报告报文的端口加入到IP组播组中；如果该报文对应的MAC组播组已经存在，但是接收报告报文的端口不在该MAC组播组中，则将接收报告报文的端口加入MAC组播组中并启动该端口的老化定时器，然后判断此报文对应的IP组播组是否存在：如果不存在，则新建IP组播组并把接收报告报文的端口加入到IP组播组中，如果存在则将接收报告报文的端口加入到IP组播组中；如果该报文对应的MAC组播组已存在，并且接收报告报文的端口也已经存在于该MAC组播组，则仅重置接收报告报文的端口上的老化定时器。

#### 6.6.1.4 Netcore 7224NSW 二层交换机 IGMP Snooping 的设置方法

具体操作：在“状态设置中”的“IGMP Snooping状态”框选中“Enable”，点击“确定”，如图所示。




图 6.66

## 6.6.2 组播路由端口

配置静态路由器端口后，此端口能加入到某一VLAN的组播组。“端口列表”中输入端口号，在“VID”中输入所属的VLAN，然后点击“增加”，如图所示：




图 6.67

## 6.6.3 IGMP Snooping 典型配置举例

先启动IGMP Snooping，为了实现交换机的IGMP Snooping功能，需要在交换机上启动IGMP Snooping。交换机上的路由器端口接到路由器上，其他非路由器端口则接到用户的PC机上。

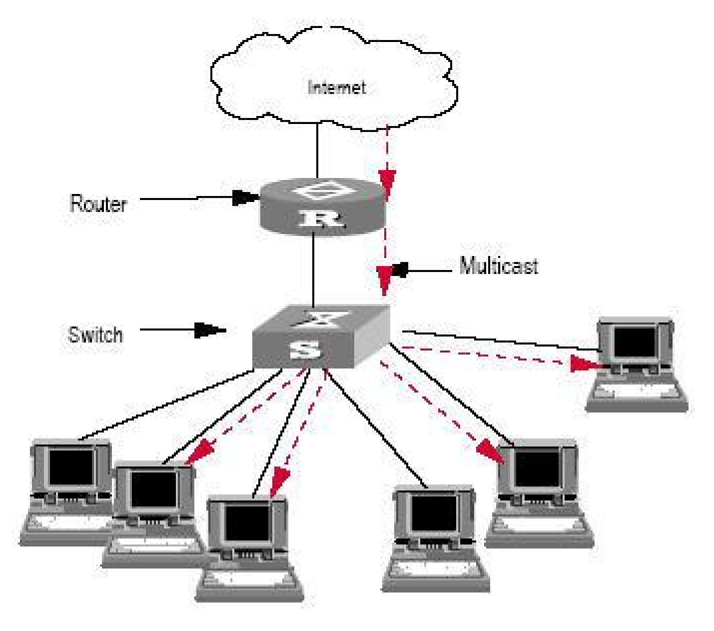



图 6.68

# 6.7 网络分析

## 6.7.1 端口分析

Netcore 7224NSW 二层交换机的端口分析功能它负责分析此端口接收的数据包、数据包的类型及数据包的速率，和发送数据包的统计。用户把数据进行分析就可以知道被统计的端口情况。

特性为用户提供了一种功能强大的故障诊断方式。该特性可以将被调查端口发送或接收的报文统计分析出来。例如连接端口 1 的工作站发生故障，对端口作分析。在不中断和介入当前报文流的情况下可以进行故障诊断。

如要对端口 1 进行分析，就在“查看端口号”选择“Port 1”，点击“确定”。如图所示：

端口分析

| 输入端口号 |
| --- |
| 查看端口号： Port1 |
| 确定 |

| 查看端口分析 | | | |
| --- | --- | --- | --- |
| 统计项目 | 总计 | 平均值/S | 最大值/S |
| 发送包总字节: | 0 | 0 | 0 |
| 发送包总数: | 0 | 0 | 0 |
| 接收包总字节: | 0 | 0 | 0 |
| 接收包总数: | 0 | 0 | 0 |
| 接收单播包数: | 0 | 0 | 0 |
| 接收組播包数: | 0 | 0 | 0 |
| 接收广播包数: | 0 | 0 | 0 |
| 接收/发送64字节包数: | 0 | 0 | 0 |
| 接收/发送65-127字节包数: | 0 | 0 | 0 |
| 接收/发送128-255字节包数: | 0 | 0 | 0 |
| 接收/发送256-511字节包数: | 0 | 0 | 0 |
| 接收/发送512-1023字节包数: | 0 | 0 | 0 |
| 接收/发送1024-1518字节包数: | 0 | 0 | 0 |
| 接收64字节以下正确包数: | 0 | 0 | 0 |
| 接收1518以上正确包数: | 0 | 0 | 0 |
| 接收64字节以下错误包数: | 0 | 0 | 0 |
| 接收1518以上错误包数: | 0 | 0 | 0 |
| 刷新 | | | |

图 6.69

如果用户收到了 64 字节以下、1518 字节以上的数据包，不管收到的是正确的包还是错误的包，都证明网络有问题，因为正常情况下，网卡不可能接收到小于 64 字节的、大于 1518 字节的数据包。但是如果是千兆网卡的话，允许接收到大于 1518 字节的包。

所以用户可以根据端口的分析来查看本网络数据包的正确性。

## 6.7.2　端口镜像

端口镜像提供端口监视功能，它把指定端口的数据包复制到监控端口。允许用户自行设置一个监视管理端口来监视被监视端口的数据。监视到的数据可以通过 PC 上安装的端口监视软件反映，如 EtherPeek NX、SpyNet 等，用户把监视到的数据进行分析就可以知道被监视端口情况，从而进行网络检测、监控和故障排除。

设置端口 1 去监视从端口 5 出去数据到端口 6 进来的数据：

具体操作：在流量捕获配置下，“捕获状态”设置为“Enable”，“捕获端口”框选中“Port1”，点击“确定”。然后在“被监视源端口列表”输入“5”，在“被监视目的端口列表”输入“6”，

点击“增加”，查看捕获器中会显示配置的条件。如图所示：

端口镜像

| 流量捕获配置 | |
|---|---|
| 捕获端口： | Port1 |
| 捕获状态： | Enable |
| 确定 | |

| 镜像端口配置 | |
|---|---|
| 被捕获源端口列表 | 被捕获目的端口列表 |
| 5 | 6 |
| 确定 | |

图 6.70

# 第七章 常见问题和处理方法

## 7.1 开机故障

### 7.1.1 电源故障

首先查看交换机的电源指示灯，如果指示灯熄灭，可能是外电源连接不良，请确定电源接线板供电是否正常，并检查电源线与电源接线板、以及与 Netcore 7224NSW 交换机的连接是否稳定可靠。

### 7.1.2 交换机启动故障

如果不能从 CONSOLE 端口连接的终端屏幕上观察到交换机成功启动，请按下列步骤检查：

- 检查所使用的终端软件设定的串口号是否正确：通常PC上带有2个串口，分别是COM1和COM2；
- 检查所使用的终端软件的通讯配置是否是：9600bps、8数据位、1停止位、无奇偶校验、无流控；
- 检查PC上的串行口工作是否正常：可以使用串口鼠标来检测串口硬件有没有故障；
- 确认用户的Windows操作系统中有没有其他程序在使用该串口；Windows操作系统不允许多个程序同时使用一个串口；

## 7.2 以太链路故障

### 7.2.1 概述

以太链路故障可能体现出多种现象：

- 无法和PC网卡连接，链路状态指示灯显示不能正常连接；
- 端口可以与PC网卡连接（链路状态指示灯正常），但无法和其他某些端口通讯；
- 端口可以与PC网卡连接（链路状态指示灯正常），但通过该端口无法对Netcore 7224NSW交换机进行管理。
- 可以把这类故障大致分为两大类型：
  1：Link-Error，链路两端无法建立物理连接，表现出的现象是链路状态指示灯不正常。
  2：配置冲突，表现出的现象是链路状态指示灯正常，但无法和其他端口进行通讯。

### 7.2.2 链路状态指示灯显示不正常(Link-Error)

出现这种情况时，请按照下列步骤进行检查：

- 查看链路另一端是否良好地连接到PC网卡或其他以太接口上；

- 检查连接电缆及两端的RJ45接头是否有锈蚀或损坏；
- 使用WEB方式(检查该端口的通讯配置（双工、速度），确定其配置是否与链路另一端相匹配。


**重要提示**

当链路两端均强制设置双工和速度时，如果设置不匹配，是无法建立连接的。

### 7.2.3 链路状态指示灯显示正常但无法通讯

出现这种情况时，请按照下列步骤进行检查：

- 使用WEB方式（见端口状态查询）检查该端口是否被停止，如果显示该端口被停用，则使用WEB方式（见端口配置中的关闭/打开）打开该端口；
- 使用WEB方式检查该端口是否在VLAN设置中与其他端口隔离；端口只能和同一个VLAN内的成员端口进行通讯。

## 7.3 无法远程登陆管理交换机

### 7.3.1 概述

请按照下面的步骤对 Netcore 7224NSW 交换机进行检查：

- 按照7.1.2 交换机启动故障介绍的方法检查Netcore 7224NSW交换机是否成功启动；
- 按照7.2 以太链路故障介绍的方法检查有无链路故障；
- 使用PING程序检测Netcore 7224NSW交换机有无回应：如果没有回应，则检查Netcore 7224NSW交换机和PC的IP地址配置是否正确；如果有回应，则可根据HTTP/TELNET连接反馈信息来判断故障原因。

### 7.3.2 检查 IP 地址设置

请按照下面的步骤对 Netcore 7224NSW 交换机进行检查：

- 检查PC的IP地址、子网掩码以及默认网关设置是否是你期望的设置：在Windows命令行方式下输入ipconfig查看PC的IP地址配置；
- 检查Netcore 7224NSW交换机的IP地址、子网掩码以及默认网关设置是否是你期望的设置：在CONSOLE方式下使用检查Netcore 7224NSW交换机的IP地址设置；
- 检查PC和Netcore 7224NSW交换机的IP地址是否被其它设备占用；

### 7.3.3 检查远程登录帐号

用户使用 WEB 或 TELNET 方式远程登录时，如果 Netcore 7224NSW 交换机连续要求输入帐号和密码，这可能是输入的帐号不存在或输入的密码错误。



**温馨提示**

控制台（CONSOLE）模式的配置方法、远程登录（Telnet）模式的配置方法，请查阅7224NSW用户手册。

# 附 录

## 附录 A 配件清单

检查包装盒里应有以下配件：

- 一台Netcore 7224NSW
- 一根串口线
- 一个电源线
- 一本用户手册
- 一张Netcore保修卡



温馨提示

如果发现物品有损坏或者遗漏，请及时与当地Netcore经销商联系。

## 附录 B FCC 认证

本设备已经进行过检测，符合 FCC 第 15 部分中的 B 级数字设备标准。该标准详细规定了安装于居住环境的无线设备可能产生的有害干扰的各项安全参数。

本设备产生、使用，并发射一定频率的无线电波。如果违反说明书中的要求进行安装，可能会造成有害的无线电干扰。但是，也不保证某种安装状态一定不产生干扰。如果本设备确实对收音或电视产生了干扰，并且通过关闭或打开本设备确认了此干扰的存在，用户可以尝试通过以下方式来减小干扰：

- 调整接收天线的位置和方向；
- 加大接收天线与本设备之间的距离；
- 将本设备接入与被干扰设备不同的电源插座；
- 咨询经销商或者有经验的收音/电视技术人员，以获取帮助。

为确保符合 FCC 对辐射的规定，应使用干扰屏蔽连接线进行连接。

在未经相关权威机构明确认可的情况下，应避免任何对本产品的改动或调整。

本设备符合 FCC 第 15 部分的规定。其操作符合以下两种情况：

- 此设备不会造成有害干扰；
- 此设备可以抵抗自身受.到的干扰，包括可能引起操作错误的干扰。

# 附录 C　技术支持

**技术支持**

支持中心电话：400-8101616
网地：http://www.netcoretec.com
E-mail： support@netcoretec.com
周一到周五，早09：00---晚19：00
周六，早10：00---晚17：00